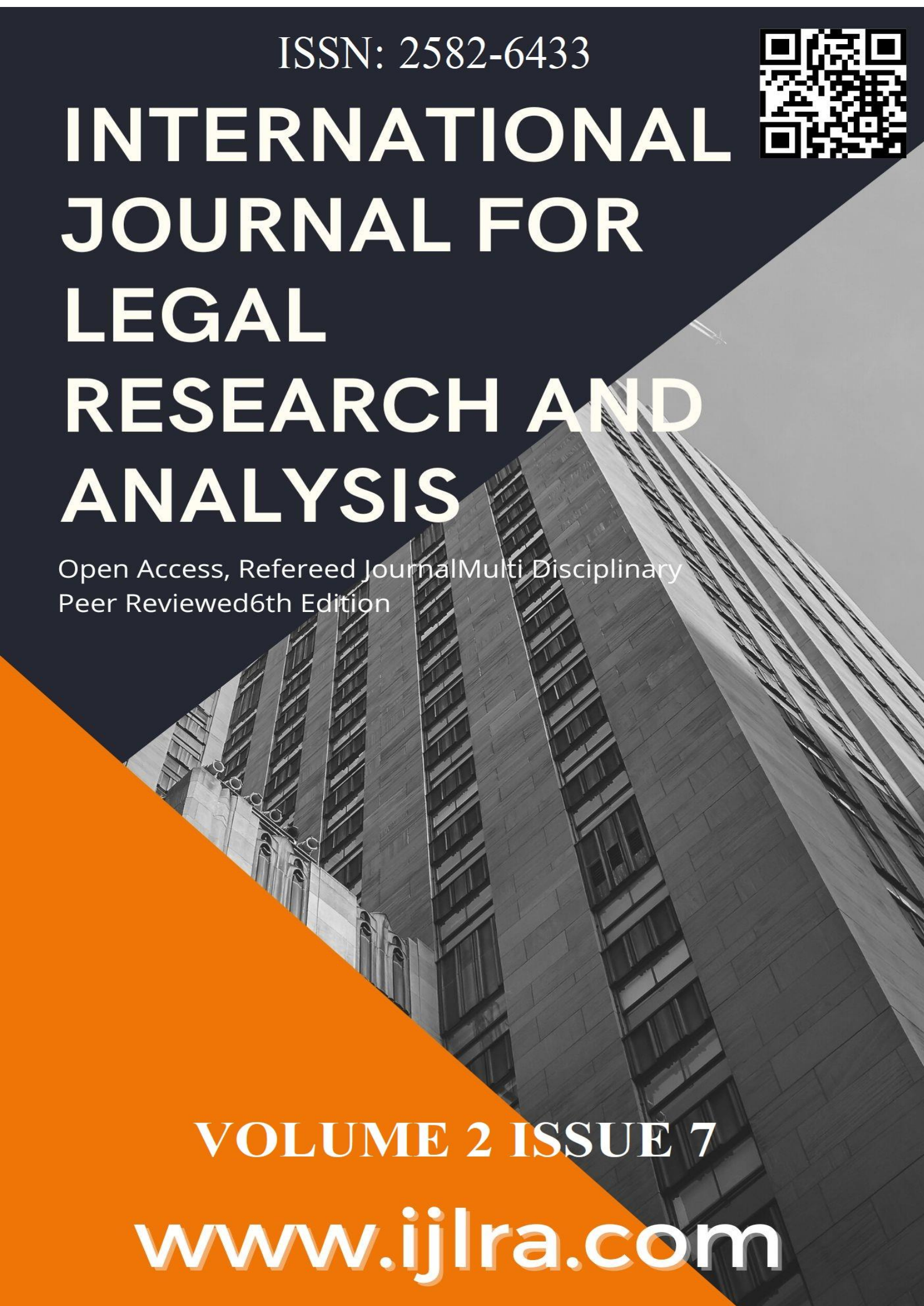
ISSN: 2582-6433

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed6th Edition



VOLUME 2 ISSUE 7

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions ofthe authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume 2 Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner whatsever for any consequences for any action taken by anyone on the basis of information in the Journal.

Copyright © International Journal for Legal Research & Analysis

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

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

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

Dr. Samrat Datta

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

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

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

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

Mrs.S.Kalpana

Assistant professor of Law

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

Avinash Kumar

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

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

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

www.ijlra.com
Volume 2 Issue 7 | April 2023
ISSN: 2582-6433

CYBER CRIMINOLOGY IN THE DIGITAL WORLD

AUTHORED BY - MUGESH S[1]

ABSTRACT:

Computer technology's ever-increasing connectivity has brought the world closer together. We can connect to the rest of the world if we have a computer and a modem. Today, a simple mobile phone is sufficient to connect you to people all over the world. Social media networking has impacted peoples' cultural, economic, and social lives over the past decade, becoming an essential part of everyone's life. These social networking sites attract users from all walks of life and store their data in the cloud, resulting in illegal data theft by cyber criminals. The general classifications of this computer related crimes include Stalking, Hacking, Web-Jacking, E-mail bombing, Computer vandalism, Cyber-terrorism etc. Because of their anonymity and low chances of detection, cyber offenders are misusing computer technology to commit a variety of crimes that must be prevented by effective legal and regulatory measures. The author in this paper attempts to explain about the concept of cyber criminology in the digital world and provides for various preventive measures available.

Key words: *Cyber-crimes, Computer, Technology, Internet, Society.*

Introduction:

According to Statista, as of January 2021, there are 4.66 billion active internet users across the globe i.e., 59.5 percent of the global population. Out of this, 92.6 percent i.e., 4.32 billion have accessed the internet via mobile devices. China, India and the United States rank ahead of all the other countries in terms of internet users. China has more than 854 million internet users, and India has approximately 560 million online users. Both countries still have large parts of the population that are offline[2]. The increasing usage of internet services results

[1] Author is an LLM Student of Department of Intellectual Property Law, SOEL, TNDALU, Chennai.
[2] Joseph John, Worldwide Digital Population as of January, 2021, (Mar 5, 2021) https://www.statista.com/statistics/617136/digital-population-worldwide/

ISSN: 2582-6433

in the danger of people being exploited by the cyber criminals. Since the past decade, social media networking has become an essential part of everyone's life affecting cultural, economic and social life of the people. These social networking sites are attracting users from all walks of life and keeping the user's data in the cloud resulting in the illegal data theft by the cyber criminals. These crimes cover a wide range of illegal computer-related activities such as theft of communication services, industrial espionage, dissemination of pornographic and sex offensive material in cyber-space, electronic money laundering and tax evasion, electronic vandalism, terrorism and extortion, tele-marketing frauds, illegal interception of tele-communication etc.

Willie Sutton, a notorious American bank robber of a half century ago, was once asked why he persisted in robbing banks. "Because that's where the money is," he is said to have replied[3]. The theory that crime follows opportunity has become established wisdom in criminology; opportunity reduction has become one of the fundamental principles of crime prevention. The same applies to computer related crimes also.

Crime: Meaning and Definition:

A crime is an act punishable by law, as being forbidden by statute or injurious to the public welfare.

According to Bentham, "offences are whatever the legislature has prohibited for good or for bad reasons. If the questions relate to theoretical research for the discovery of the best possible laws according to the principle of utility, we give the name of offence to every act which we think ought to be prohibited by reasons of some evil which it produces or tends to produce"[4].

Cyber Crime: Meaning and Definition:

The term 'Cyber Crime' is nowhere defined, this concept is varied because the crime which is going to be committed by using any means of communication or internet can be termed as a cybercrime. A cyber crime may be defined as any criminal activity that uses a computer

[3] Peter Grabosky, Computer Crimes in a World Without Borders, (Mar 13, 2000) https://www.crime-research.org/library/Peter.htm
[4] Divya19, Cyber Crime - A Hindrance In Digital World, http://legalserviceindia.com/legal/article-3210-cyber-crime-a-hindrance-in-digital-world.html

ISSN: 2582-6433

either as an instrumentality, target or means of perpetrating further crime. In other words, cyber crime is an unlawful act wherein the computer is either a tool or a target or both.

In a sense, it is not radically different from the concept of conventional crime insofar as both include conduct whether act or omission, which causes breach of law and therefore, it is punishable by the state.

Constitutional View:

Hacking into someone's private property or stealing someone's intellectual work is a complete violation of his right to privacy. The Indian constitutional does not specifically provide the "right to property" as one of the fundamental rights guaranteed to the Indian citizens but it is protected under Indian penal code. Right to property is an important natural need of every human being as it creates boundaries is around an individual where the other persons entry is restricted. The right to privacy prohibits interference in other private life. The apex court of India has clearly affirmed in its Judicial pronouncements that right to privacy is very much a part of the fundamental right guaranteed under Article 21 of the Indian Constitution. Thus, right to privacy or its personal stuff then the accused can be challenged of violation of article 21[5] of Indian Constitution and prescribed remedy can be invoked against the accused.

Typology of Cyber Crime:

Cyber crimes may broadly be classified into two major categories :—

1. Cyber crime where computer is itself a target of the crime; and
2. Cyber crime where computer is an instrument of the crime.

1. Computer as a target of the crime:

In this category of cyber crime, computer itself is a target of the crime. These crimes generally include :-

(i) sabotage of computer systems or computer networks;

(ii) sabotage of operating systems and programmes;

(iii) theft of data/information;

[5] Article 21 of the Constitution of India, 1950.

ISSN: 2582-6433

(iv) theft of intellectual property, such as computer software;

(v) theft of marketing information; and

(vi) blackmailing based on information gained from computerised files such as personal history, sexual preferences, financial data, medical information etc.

2. Computer as an Instrument Facilitating Crime:

In this category of crime, the computer is used as an instrument to commit the crime. The terrorists and criminals are using Internet methods such as e-mail to flesh out encrypted messages around the world. In these crimes, computer programs are manipulated to facilitate the offence. For example, fraudulent use of Automated Teller Machine (ATM) cards and accounts, frauds related to e-banking or e-commerce, electronic data-interchange etc. are committed by using computer. Cyber pornography, software piracy, on-line gambling, copyright infringement, trademark violations are some other illustrations of such crimes[6].

General Classification:

The general classification of cyber crimes are;

(1) Cyber crimes against persons;

(2) Cyber crimes against all forms of property; and

(3) Cyber crimes against State or society.

1. Cyber crimes against persons:

Cyber crimes against person or individual include harassment via e-mail, stalking, defamation, unauthorised access to computer systems, indecent exposures, e-mail spoofing, fraud, cheating and pornography etc.

2. Cyber crimes against all forms of property:

Computer related crimes against property include computer vandalism, transmission of virus, denial of service at lack, unauthorised access over computer system, intellectual property rights violations, Internet time-theft, sale of illegal articles etc.

[6] Dr. N.V. Paranjape, Criminology & Penology with Victimology, Pg. No. 145, 15th Edition (2012).

ISSN: 2582-6433

3. Cyber crimes against State or society:

Cyber crimes against state or society may comprise possession of unauthorised information, cyber terrorism, distribution of pirated software, polluting youth through indecent exposure, trafficking financial scams, forgery, online gambling etc[7].

Some of the cyber crimes which are generally committed in the cyber space through computer systems are explained as follows :-

Stalking: In stalking, persistent messages are sent to unwilling recipients, thus causing them annoyance, worry and mental torture. Sending of unsolicited e-mails or spamming is an infringement of right of privacy. Online harassment and threats may take many forms.

Cyber stalking usually occurs with women who are stalked by men, adolescents or adult pedophiles. A cyber stalker does not have to leave his home to harass his targets and has no fear of physical avenge since he cannot be physically touched in cyber space.

In ***Burnett v. George***[8]., The plaintiff had been subjected to a series of assaults, unwanted visits, damage to her house, telephone threats and telephones calls at unsocial hours. The Court of Appeal granted an injunction prohibiting the defendant from entering her property and from assaulting, molesting r interfering with her by acts calculated to impair her health.

A cyber stalker generally collects all the personal information about the victim such as name, age, family background, telephone or mobile numbers, workplace etc. He collects this information from the internet resources such as various profiles the victim may have filled-in while opening the chat or e-mail account. The menace of cyber stalking has spread like wild-fire in India and many innocent women., girls and children are being targeted as its victim.

Hacking: Hacking is the most common form of cyber crime in these days. The reason why hackers indulge in this crime may vary from monetary gain to political interest or it may even be for the sake of sheer thrill. Hacking may be of different forms such as web-spoofing, e-mail bombing, trojan attacks, virus attacks, password cracking etc. In simple words hacking means seeking unauthorised access through computer network[9].

[7] Dr. Ajeet Singh Poonia, Cyber Crime: Challenges and its Classification, November-December 2014, https://www.ijettcs.org/Volume3Issue6/IJETTCS-2014-12-08-96.pdf.
[8] Burnett v. George., (1992) 1 FLR 525.
[9] Hacking is an punishable offence under The Information Technology Act, 2000 with imprisonment up to 3 years and fine u to rupees 1 crore for unauthorized access. It is also punishable under Section 66 of the Copyright Act with imprisonment up to 3 years and fine up 2 lakhs rupees.

ISSN: 2582-6433

Web-jacking as a specie of hacking is nothing but forcefully taking over control of a website of someone else or the victim. The motive is usually ransom or attainment of some illegal political purpose.

E-mail bombing means sending large number of mails to the victim which may be an individual or a company to cause confusion and harassment.
Trojan is an unauthorised programme which gains control over another's system by representing itself as an authorised programme.

The administrator of any website has a password and a username, then only he may use to upload files from his computer on the Webserver where his website is hosted. This password remains secret with the administrator. If a hacker gets hold of this username or password, then he can pretend to be the administrator. Computer hackers may affect the commercial websites or e-mail systems thus paralysing the entire business.

Under Indian law it has been clearly laid down in ***Smt. Mathri v. State of Punjab***[10]., that for establishing the offences of criminal trespass it is not enough to merely show that the person entering upon the property of another had knowledge that his act would cause annoyance. The rule that a person must be presumed to intend the natural consequences of his act is not a binding rule, if any other intention can be shown. This interpretation may be problematic while dealing with crimes on the Internet.

E-mail spoofing: A spoofed e-mail may be said to be one which misrepresents its origin. That is, it shows its origin to be different from which it actually originates. For example, where A sends a threatening e-mail to the President of the student union threatening to detonate a nuclear device in the college campus and this e-mail was sent from the account of some other student, 'A' would be guilty of e-mail spoofing.

Computer Vandalism: Literally speaking, vandalism means destroying or damaging property of another. In the context of cyber crime, computer vandalism includes within it any kind of physical damage done to the computer of any person. It may be in the form of theft of a computer or some part thereof or a peripheral attached to a computer.

[10] Smt. Mathri v. State of Punjab., AIR 1964 SC 986 (India).

ISSN: 2582-6433

Cyber Terrorism: According to U.S. National Infra-structure Protection Center, cyber terrorism is defined as,

"a criminal act perpetrated by the use of computer and telecommunication capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government population to conform to a particular political, social or ideological agenda[11]."

In *Mohammed v. State of Gujarat*[12]., In this case a Chief Minister of a State was threatened with life through email. A case was filed under Section 507[13] of Indian Penal Code, 1860 and Section 67[14] of Information Technology Act, 2000. Quashing the charge under Section 67, the High Court observed that "Nothing in the said e-mail can be stated to be obscene or such material as can be categorized as lascivious or such which would deprave or corrupt person's mind who may have accend to such mail. Ex-facie offence under section 67 is, therefore, not made out. The said provision is, therefore, required to be deleted against the petitioner.

Cyber terrorism has domestic as well as international ramifications. It may be defined as the premeditated use of disruptive activities or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives. A 'cyber terrorist' may be defined as a person who uses computer system as a means to achieve any of the following objectives :-

(i) putting the public or any section of the public in fear; or
(ii) affecting adversely the harmony between different religious, racial, language or regional groups or castes or communities; or
(iii) coercing or overawing the government established by law; or
(iv) endangering the sovereignty and integrity of the nation.

Cyber Pornography: Pornography on the internet may take various forms. It may include hosting of website containing some obscene or prohibited material or use of computers for producing obscene materials. Such material tends to pervert the thinking of adolescents and corrupts their mind set. A person who publishes or transmits or causes to be published in the

[11] Pragati Ghosh, Short Essay on Cyber Terrorism https://www.shareyouressays.com/essays/short-essay-on-cyber-terrorism-458-words/121708.
[12]Mohammed v. State of Gujarat., in SCR.A/1832/2009
[13] Section 507 of the Indian Penal Code, 1860.
[14] Section 67 of the Information Technology Act, 2000.

ISSN: 2582-6433

electronic form any material which is lascivious, or if its effect is such as to tend to deprave or corrupt the persons who are likely to see, read or hear the matter contained or embodied in it, is liable to punishment which may extend to imprisonment upto five years and with fine, which may extend to rupees one lakh[15]. The important ingredients of such an offence are publication and transmission through any electronic medium, of pornographic material, in any electronic form.

In ***Prakash v. State of Tamil Nadu***[16]., Where appellant has been served detention order primarily on grounds that he has committed offences under section 67[17] of Information Technology Act, 2000, under section 4 and 6 of Indecent Representation of Women (Prohibition) Act, 1986[18], and under section 27[19] of Arms Act, 1959 and the detaining authority admittedly took note of a letter from a women member of the public stating that appellant had been involved in heinous crimes, that police, should ensure he is punished and not released on bail, held on facts, contents of letter were not extraneous or irrelevant.

Cyber Defamation: Cyber defamation is not different from conventional defamation except that it involves the use of cyber space medium. Any derogatory statement which is intended to injure a person's name or reputation on a web-site or sending e-mail containing defamatory information to some other person constitute the offence of cyber defamation.

E-mail Frauds (Spam): E-mail is an inexpensive and popular device for distributing fraudulent messages to potential victims. This technique not only helps to assume someone else's identity, but also helps to hide one's own. Therefore, the person committing the e-mail has little chance of being detected or identified. The most common e-mail fraud is 'phishing' i.e., personal information fraud. The purpose of such spams is to trick the person for divulging his personal information so that the offender can steal his identity and commit crime in that person's name. Section 74[20] of the Copyright Act makes internet fraud as an offence punishable with imprisonment upto two years or with fine which may extend to rupees one lakh.

[15] Section 67 of the Information of Technology Act, 2000.
[16] Prakash v. State of Tamil Nadu., (2002) 7 SCC 759 (India).
[17] Section 67 of Information Technology Act, 2000.
[18] Section 4 and 6 of Indecent Representation of Women (Prohibition) Act, 1986
[19] Section 27 of Arms Act, 1959.
[20] Section 74 of the Copyright Act.

ISSN: 2582-6433

Money Laundering: It is a kind of cyber crime in which money is illegally downloaded in transit. There is a phenomenal increase in the incidence of this cyber offence. Out of 146 seizures made by the Enforcement Directorate in money laundering cases in the year 2005 recoveries were made in 106 cases involving seizure of about 9.5 crores of rupees.

Data diddling: This offence involves changing or erasing of data in subtle ways which makes it difficult to put the data back or be certain of its accuracy. This is resorted to for the purpose of illegal monetary gains or for committing a fraud or financial scam[21].

Cyber Crime Beyond Boundaries:

Cyberspace is a digital medium and not a physical world. It is limitless, constantly changing its shape, attributes and characteristics. With computers and computer networks, one can easily connect to the world in a split second. The internet has made the world smaller, bringing countries, people and businesses close together. Computer devices have become smaller and portable and are able to carry large amount of data/information across the globe. The ever-increasing connectivity of computer technology has brought the world closer. With access to a computer and a modem, you are connected to the world. Today a simple mobile phone is enough to connect you to people in other parts of the world[22].

In ***Daya Singh Lahoria v. Union of India***[23]., It was held that a fugitive criminal, if extradited into India under an extradition decree, could be tried only for the offences mentioned in the extradition decree and for no other offences and the criminal courts of India would have no jurisdiction to try such fugitive for any other offences.

Determining which country has jurisdiction for the purposes of a criminal prosecution may establish whether the conduct would be a crime, how the crime would be defined, and how it would be punished. First, the absence of a geographical boundary for commission of the crime; second, the glaring lacuna in the legal arena with the lack of a settled law thriving internationally and the existence of conflicting laws; third, the existence of either positive juridical claims where many countries claim to exercise jurisdiction and the negative juridical claims where there is no claim for jurisdiction by a single country, resulting in crimes going

[21] Vardhaman Mahaveer Open University, Kota, Study Material, http://assets.vmou.ac.in/PGDCL04.pdf.
[22] Justice Surya Kant, Cyber space and jurisdictional concerns, https://ujala.uk.gov.in/files/ch3.pdf.
[23] Daya Singh Lahoria v. Union of India., (2001) 4 SCC 516 (India).

ISSN: 2582-6433

unpunished[24].

In ***The People of the State of New York vs. Gaming Corporation***., [25]an online gaming company based in Antigua (where online gambling is legal) maintained corporate offices in New York, a state where online gambling is illegal. The issue in this case was whether the State of New York could bring the online gambling company under its jurisdiction and prosecute it for offering gambling to internet users in the state. The court held that the State of New York had the jurisdiction to prosecute the gambling company as it was in persona located in New York, and thus came within the jurisdiction of a competent court in New York.

Cyber crime Prevention Strategies:

Laws are generally meant for meeting the needs of the society and it is, therefore, a dynamic concept which undergoes changes with the changing need of the society. Because of the anonymity of its character and negligible chances of being detected, the cyber offenders are misusing the computer technology for committing a variety of crimes which need to be prevented by an effective law and regulatory measures.

Preventive Measures Provided by the Government:

1. **Legislative Measures:**
    1. Special Statutes on cyber crimes against women is required to be passed to deal with the all form of cyber crime against women.
    2. Statutes and laws made by the legislative related to cyber crime against women must be based on mental harm than the physical harm as till now it is made more of physical harm.
2. **Judicial Suggestions:**

Alike various tribunals, a special bench for dealing with cyber crimes against women may be created atleast in each and every High Court. Special branch may also be created in every metropolitan cities and districts.

3. **Suggestions to protect women from getting victimized:**

1. Always use strong passwords and don't share password it may sound pointless. As nobody in their sight mind share their password, right? Wrong any person may have

[24] Nandhan Kamath, Law Relating to Computers, Internet & E-commerce, Pg. No. 23, 5th Edition (2017).
[25] The People of the State of New York vs. Gaming Corporation 714 NYS 2d 844 (USA).

ISSN: 2582-6433

shared their password with a trusted friend or partner. While friends may not intentionally cause you harm, they may accidentally reveal your password to someone. Sometimes relationship change before your password does. So, it is very necessary to keep passwords private as well as complicated.

2. Don't always share more than mandatory
3. Don't reveal everything: always be careful about posting details about your activities.
4. Simply block people you don't want to interact with.
5. The very important point is that every women must report any such cyber crime without any limitations.
6. Don't share any photos anywhere in the social media.
7. Don't meet online friends anywhere alone[26].

Future Progress in Cyber Space:

The pace at which cybercrime is growing is one of the most disturbing trends. Valerie McNiven, a U.S. Treasury Advisor, has proclaimed "Last year was the first year that proceeds from cybercrime were greater than proceeds from the sale of illegal drugs, and that was, I believe, over $105 billion." She further added that "cybercrime is moving at such a high speed that law enforcement cannot catch up with it." It seems clear that the issue will only become worse in the next few years, now that professionals have realized the potential windfalls if exploited properly.

With professional criminals managing the money laundering and organization of such schemes, it begs to ask where all the technical know-how will come from in order to perform cybercrime. Unfortunately, there are growing numbers of intelligent black-hats with university degrees spread around the globe, many of them operating in countries where legal employment does not pay as well and the chances of being caught are slim. But more troublesome is that it has become easier than ever before to be a hacker capable of inflicting great harm on networks and committing cybercrime. The future of the Internet is still up for grabs between criminals and normal users. Whether cybercrime is still a pertinent issue ten years from now is unknowable in a sense, but if the Internet will continue to grow, it must be solved so that the realities of

[26] Sanjeev Kumar & Priyanka, Cyber Crime against women: Right to Privacy and other issues, October 2019, https://www.researchgate.net/publication/344153821_CYBER_CRIME_AGAINST_WOMEN_RIGHT_TO_PRIVACY_AND_OTHER_ISSUES.

ISSN: 2582-6433

cybercrime will be proportional to real-world crimes, if not better[27].

Conclusion:

Cyber crime has high potential and thus creates high impact when it is done. It is easy to commit without any physical existence required as it is global in nature due to this it has become a challenge and risk to the crime fighter and vice versa. The borderless nature of ICTs may not allow for rigid regulations and instead challenges the principle of criminal laws. As such, international laws and regulations combined with reliance on technologies are crucial to counter the crime race. The preventive measures should be taken to prevent the society as well as the organizations from the cybercrimes instead of avoiding the uses of the technology.

[27] Sumanjit Das and Tapaswini Nayak, Impact of Cyber Crime: Issues and Challenges, October 2013, https://www.ijeset.com/media/0002/2N12-IJESET0602134A-v6-iss2-142-153.pdf.