Quest Journals
Journal of Research in Humanities and Social Science
Volume 10 ~ Issue 1 (2022)pp: 12-23
ISSN(Online):2321-9467
www.questjournals.org

Research Paper

Cyber Crime and Human Rights

Ms Riya Agarwal
Student of BALLB (Hons) 10th Sem
Seeding School of Law and Governance
Jaipur National University, Jaipur

Ms Bhavana Ladha
Student of BALLB (Hons) 10th Sem
Seeding School of Law and Governance
Jaipur National University, Jaipur

ABSTRACT
Human rights are the rights which are provided to an individual by honour of him being a human being. These are the rights which a human being can enjoy everywhere irrespective of online or offline space .This paper includes how the point of global concern arises when we talk about safeguarding human rights in cyberspace and it also includes the constitutional and the criminal liability arises out of Indian national law. When we talk about human rights and cyberspace, we also talk on the issue of cybercrimes. Crimes which are done on the internet or by making the internet a medium are known as cyber-crimes. Many times cyber criminals perform such crimes which violate the human rights of the individuals, women and children being the weaker link cause great impact on their mental and physical health. Lack of jurisdiction and regulatory bodies with strict law make it a global issue. India being the third world nation has its own challenges to curb out the crime, lack of strict domestic laws makes it more challenging. Thus the human rights on cyberspace are violated in both the ways, by crimes and by various application of laws .

KEYWORDS:- *Human rights, cybercrime, cyberspace, women and children, international organization, law, internet and hacking .*

***R**eceived 04 Jan, 2022; **R**evised 13 Jan, 2022; **A**ccepted 15 Jan, 2022 © The author(s) 2022.*
P**ublished with open access at **www.questjournals.org

I. INTRODUCTION

Human Rights in cyber space is a new field of global concern. With the advent of the internet and the popularity which it has gained in the recent years, it is necessary to monitor the cyber space and protect the human rights of people using it. The internet has given birth to a new category of criminals i.e., cyber criminals. The cyber criminals are intruding into the private lives of the individuals thereby infringing the human rights of the internet users. The internet is a strong medium of expression of our ideas and thus it should be without any restrictions. It provides us a platform to exercise the right to freedom of expression and information.

Back in the time when the internet came into existence and technology was still thriving no one would have ever thought that it can affect their fundamental rights to such extent. There was a time when wealth was counted by the amount of money people had in their bank accounts but in today's world, it's all about information. Hence it is said, "information is wealth".

Cyber space can be defined as an intricate environment that involves interactions between people, software and services[1]. It makes the place vulnerable as well as crucial. Where technology is providing us a helping hand in evolving our laws and the society, it'sexcruciatingly becoming a well-known platform of human rights infringement.

[1] http://docs.manupatra.in/newsline/articles/Upload/C4971E8F-86E8-48E1-886B-CEF0B774397F.pdf

Human rights are at stake when government engage in cyberattacks, like when Russia shut down the internet, as it did in Crimea in2016 and in Ingushetia in 2018, or when a government hacks into a dissident or journalist's phone, as Saudi Arabia and the UAE have repeatedly done[2].

The technologies relevant to infringements of human rights include: the Internet, DNA analysis techniques, biometric identification technologies, CCTV and mobile phone cameras, listening devices, networked databases and neural networks for data analysis, voice recognition systems and others[3].

A recent report commissioned by IBM puts the global average cost of a data breach to a company in 2020 at USD 3.86 million.[4]The main cause behind such awful conditions is the non-existence of proper laws in various countries around the globe and the lack of adequate authorities to manage the situation. Trusting over authorities with biometrics and personal information makes them responsible for every data they lose. It holds them liable to invade privacy and security.

In May, 2020 the UN Security Council had its discussion over cybersecurity and the need to recognize cyber-attacks as one of the human rights issues. The course of action detailed moves such as Internet shutdowns by the government and hacking into devices of dissidents, can lead to serious violation of human rights. The idea was acknowledged by at least a dozen countries including Estonia, Belgium, the Netherlands, Ecuador, Japan, Switzerland, and others[5].

WHAT ARE CYBER CRIMES AND HUMAN RIGHTS ?

Merriam Webster defines "**crime**" as an illegal act for which someone can be punished by the government, especially a gross violation of law. The act is forbidden by the government as per their national or international laws.

Cyber Crime– Cyber crime is any criminal activity in which a computer or network is the source, target or tool or place of crime. According to The Cambridge English Dictionary cyber crimes are the crimes committed with the use of computers or relating to computers, especially through the internet. Crimes which involve use of information or usage of electronic means in facilitating crime are covered under the ambit of cyber crime.Cyber crime also known as the computer crime is the use of an instrument for illegal ends, such as committing fraud, trafficking in child pornography, and intellectual property, stealing identities or violating privacy.[6] Cybercrime is progressing at an incredibly fast pace, with new trends constantly emerging.[7]

Junaid Sorosh-Wali, Officer-in-Charge, Head UNESCO National Office for Palestine, stated in his opening remarks: How to tackle the challenges of online terrorism, money laundering, and illegal online content, without putting human rights such as freedom of expression at risk, is the delicate balancing act that today's discussions will cover. He emphasized that ensuring the right to unhindered speech online and the free flow of information, while protecting Internet users from the real threats they face, should be at the heart of any attempt to combat online cybercrime.[8]Cybercrimes can be committed against almost anyone, anywhere in the world by almost anyone anywhere in the world. Not only does this often make it difficult to track down the perpetrators of the crime, but even if they are found it raises questions as to who is responsible for prosecuting the crime if it is even determined to be a crime.[9]. Cybercriminals are becoming more agile, exploiting new technologies with lightning speed, tailoring their attacks using new methods, and cooperating with each other in ways we have not seen before.[10]Complex criminal networks operate across the world, coordinating intricate attacks in a matter of minutes.Cyber crimes are committed in different forms. In the matters of cyber crime India is also not far behind the other countries where the rate of incidence is increasing day by day. 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. Therefore it stands to reason that cyber crimes are offences related to computers, information technology , internet and virtual reality .

[2] https://www.hrw.org/news/2020/05/26/its-time-treat-cybersecurity-human-rights-issue
[3] http://www.cybercrimejournal.com/smithijccjuly2007.pdf
[4]Cost of a Data Breach Report, 2020; https://securityintelligence.com/posts/whats-new-2020-cost-of-a-data-breach-report/
[5] "It's Time to Treat Cyber security as a Human Rights Issue". Human Rights Watch. Retrieved 26 May 2020
[6]A Study on the Cyber-Crime and Cyber Criminals: A Global Problem, Volume: 03, June 2014, Pages: 172-179
[7]https://www.interpol.int/en/Crimes/Cybercrime

[8]https://en.unesco.org/news/journalists-academics-human-rights-defenders-and-government-discuss-palestinians-cybercrime-law
[9]https://www.iovation.com/topics/what-is-cybercrime-definition-and-examples-of-cybercrime
[10]https://www.interpol.int/en/Crimes/Cybercrime

The United Nation defines Human rights as, "Human rights are rights we have simply because we exist as human beings – they are not granted by any state. These universal rights are inherent to us all, regardless of nationality, sex, national or ethnic origin, color, religion, language, or any other status. They range from the most fundamental – the right to life – to those that make life worth living, such as the rights to food, education, work, health, and liberty.[11]

The Universal Declaration sets out general principles concerning physical integrity (life, liberty, arrest, detention, torture, freedom of movement, asylum), social welfare (social security, the right to work, rest, leisure, education), health, adequate standard of living, the family, legal integrity (nationality, participation in government, recognition before the law, fair trial), and mental and moral integrity (dignity, freedom of thought, conscience and religion, freedom of opinion and expression, freedom of peaceful assembly and association)[12].

The Universal Declaration of Human Rightswhich is the pioneering document in this field provides the definition of human rights in its first two articles as follows:-

"Article 1- All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood.

Article 2- Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. Furthermore, no distinction shall be made on the basis of the political, jurisdictional or international status of the country or territory to which a person belongs, whether it is independent, trust, non-self-governing or under any other limitation of sovereignty."

Right to life also includes the right to privacy. "Liberty" gives the people freedom to express themselves and the right to speak. These rights are provided with some reasonable restrictions which must be kept in mind while exercising them.

Alan F. Westin defines privacy as "the claims of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.[13] Right to privacy is a fundamental human right. It is recognised around the world in diverse regions and cultures.[14]

The United Nations Human Rights Commission has stated that "The same rights that people have offline must also be protected online" (mentioning in particular freedom of expression)[15]

"The Internet is one of the most powerful instruments of the 21st century for increasing transparency in the conduct of the powerful, access to information, and for facilitating active citizen participation in building democratic societies."[16] It has become the biggest platform where people profess their freedom of expression via pictures, captions, debates, blogs, vlogs and personal chats.

The International Covenant on Civil and Political Rights (ICCPR) states (in article 19(2)): Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

The HRC has stated that the freedoms of expression and information under article 19 of the ICCPR include the freedom to receive and communicate information, ideas and opinions through the Internet.[17]

Article 19 (3) of ICCPR states, The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:(a) For respect of the rights or reputations of others;(b) For the protection of national security or of public order (order public), or of public health or morals.

It means that 'like all technological inventions, the Internet can be misused to cause harm to others', and therefore that, as an exceptional measure, a restriction may be imposed on online content to protect the rights of others, provided it passes the strict test set out in article 19(3) of the ICCPR.[18]

The market has various actors, considering organisations, government and non- government authorities who now provide services digitally and pass out confidential information through online medium.

[11]https://www.ohchr.org/en/issues/pages/whatarehumanrights.aspx

[12]Crime Control in the Digital Age: An exploration of Human Rights Implications, Russell G. Smith, International Journal of Cyber Criminology Vol1 Issue 2 July 2007

[13]Alan F. Westin, Privacy and Freedom (1967)

[14]Cyber Privacy, Raman Mittal & Neelotpal Deka, Chapter 8, Legal Dimensions of Cyberspace

[15]Human rights and cyberspace :use and misuse, Mr. Karra Kameshwara Rao, Bharati law Review, July-Sept,2016

[16]United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue

[17]Human Rights Committee, General Comment No. 34, note 4, para 12.

[18]https://humanrights.gov.au/our-work/rights-and-freedoms/projects/human-rights-and-internet

Discriminaton on the basis of race is infringement of human right as per UN convention on Elimination of All India of Racial Discrimination (CERD) as well as definition provided by UN. Racism can take many forms, such as jokes or comments that cause offence or hurt; name-calling or verbal abuse; harassment or intimidation, or public commentary that inflames hostility towards certain groups.[19] When racial discrimination is done on cyberspace it's termed as "cyber racism". In 2008 cyber-racism was addressed in the context of racial and religious discrimination and vilification in the Commission's submission to the United Nations High Commissioner of Human Rights on combating the "Defamation ofReligions".[20]This shows the advent of the need to look into the matter of cyber racism leading to violation of human rights. The rate of fraud, defamation, and cyberbullying in countries shows that people are not aware of the dangers of cyberspace and are required to be educated with respect to cyber dangers and rules/ regulations to be able to defend their cyber human rights.[21]

Cyber Stalking, Cyber bullying, Extortion, image based sexual exploitation etc. all leads to sexual harassment on cyberspace. One in four young adults experiences harassment or abuse through technology. 52% of youth who experience digital abuse are also experiencing physical abuse. 33% of digital abuse victims said they were also sexually coerced. 84 % of digital abuse victims said they were also psychologically abused.[22] With the internet taking its roots in our daily life it is essential to hold repercussions against those who violate the dignity of their fellow beings. Sharing of private pictures to both males and females, abusive and vulgar remarks, video chatting on social media platforms often lead to sexual harassment. Cyberspace is not evil, it's the people's mindset, sharing and developing videos or circulating pictures without people's consent, Impersonating to be someone else, harassing someone with fake-id in order to take revenge or defame is cybercrime.

II. EVOLUTION & PRESENT DEVELOPMENT

"Cyber bullies can hide behind a mask of anonymity online, and do not need direct physical access to their victims to do unimaginable harm." **-Anna Maria Chavez**

Crime is both a social as well as an economic phenomenon. Its history is as old as human society. Many books right from the prehistoric days, and mythological stories have spoken about crimes committed by individuals be it against another individual like ordinary theft and burglary or against the nation like spying, treason etc. Kautilya's Arthashastra which is written around 350 BC, considered to be an authentic administrative treatise in India, discusses the various crimes, security initiatives to be taken by the rulers, possible crimes in a state etc. and also advocates punishment for the list of some stipulated offenses. Different kinds of punishments have been prescribed for listed offenses and the concept of restoration of loss to the victims has also been discussed in it.

The concept of human rights has originated from different schools of thought who are based on different religions, philosophies and different law schools. The foundation of the concept of Human Rights was laid down by all religious tradition. Human rights revolve around the notion of individual rights,justice, individual liberty and the citizenship of the people under the protection of State. The concept of the United Nations to protect human rights came into existence when the League of Nations turned out to be a complete failure leading to World War II. The organisation then took the authority and responsibility to protect human rights across the globe.

Crime in any form adversely affects all the members of society. In developing economies, cybercrime has increased at rapid strides, due to the rapid diffusion of the Internet and the digitization of economic activities. Thanks to the huge penetration of technology in almost all walks of society right from corporate governance and state administration piling up their confidential data, to the lowest level of petty shopkeepers computerizing their billing system, we find computers and other electronic devices pervading human life.

The Internet is the fastest technique on earth that one can find these days and for everything, it is the best solution that people consider looking into. It has all the benefits and advantages like communication, advertisement, online movie and songs downloads, emailing, instant messaging and searching out the concerns and issues there are plenty of things that the internet has got wrong as well.

It is rightly said that technological development in every area is likely to cause drastic effects in every walk of life. The scientific and technological advancement, especially in the field of communication and

[19]https://www.racismnoway.com.au/wp-content/uploads/2017/02/cyber_racism_factsheet2014.pdf

[20]https://humanrights.gov.au/our-work/rights-and-freedoms/projects/human-rights-and-internet

[21]Cyberbullying and Cyber Human Rights: The Case of Iran, Mehrak Rahimi; https://www.hurights.or.jp/archives/asiapacific/section1/Cyberbullying%20and%20Cyber%20Human%20Rights.pdf

[22]http://diversity.umw.edu/title-ix/files/2019/04/RCASA-Cybersecurity-Presentation-updated.pdf

information have created havoc thus, opening new vistas for the human beings including the criminals. On the other hand, legislatures have been compelled to frame exclusive enactments to deal with crimes committed with the help of concerned devices.

DEVELOPMENT OF CYBER CRIME:-To define cybercrime, we can say, it is just a combination of crime and computer. To put it in simple terms 'any offense or crime in which a computer is used is a cybercrime'. Interestingly even a petty offense like stealing or pick-pocket can be brought within the broader purview of cybercrime if the basic data or aid to such an offense is a computer or information stored in a computer used (or misused) by the fraudster.

Cyber Crime has a direct impact on human rights, particularly the right to privacy, freedom of expression and the free flow of information. There was a time when cyber- crime was merely to steal data by incrupting or hacking devices. But with passing time its boundaries are getting wider and deeper into the roots of human rights.

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 property crime, e-mail, spoofing, forgery, cyber defamation, cyberstalking, unauthorized access to Computer system, theft of information contained in the electronic form, e-mail bombing, physically damaging the computer system etc. In a cybercrime, computer or the data itself is the target or the object of offense or a tool in committing some other offense, providing the necessary inputs for that offense. All such acts of crime will come under the broader definition of cybercrime.

In the past, cybercrime has been committed by individuals or small groups of individuals. However, we are now seeing an emerging trend with traditional organized crime syndicates and criminally minded technology professionals working together and pooling their resources and expertise. Cybersecurity Ventures predicts cybercrime will cost the world in excess of $6 trillion annually by 2021, up from $3 trillion in 2015.[23]

GLOBAL PERSPECTIVE:- According to General Assembly resolution and Commission on Crime Prevention and Criminal Justice resolutions the Global Programme on Cybercrime is mandated to assist Member States in their struggle against cyber-related crimes through capacity building and technical assistance. Cybercrimes often challenge the effectiveness of domestic and International law. China and United States Corporation is one of the most striking progress recently because they are the top two source countries of cybercrime. The recent pace in usage of the internet across the globe lead to gigantic problems of data stealing and system encryption via viruses and malwares affecting the privacy and security of countries and organisations. Cybersecurity Ventures predicted that cybercrime will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, and will be more profitable than the global trade of all major illegal drugs combined.[24] Chronological order of various such events occurring in 2020 can derive the clear picture of how 2021 is going to be a drastic year ahead.

January 2020 - Mitsubishi announces that a Chinese group had targeted the company as part of a massive cyber-attack that compromised personal data of 8,000 individuals as well as information relating to partnering businesses and government agencies, including various projects dealing with defence equipment .

February 2020 - The U.S. DISA (Defense Information Systems Agency) announced that it had suffered a huge data breach exposing the personal information of an enormous number of individuals.

February 2020 - Russia is accused by more than 10 countries for a series of cyber-attacks against Georgia in 2019 that lead to thousands of private, media, organisations and state institutions' websites offline.

March 2020 - Chinese hackers have targeted over 75 organizations around the world in the manufacturing, media, healthcare, and non-profit organisations who are part of a broad ranging cyber practice of spying campaigns.

[23]2020 Official Annual Cybercrime Report by Cybersecurity Ventures; https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/

[24]https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/; Cybersecurity Ventures Official Annual Cybercrime Report, 2020

April 2020 - Suspected Vietnamese government hackers used intentionally harmful apps uploaded to the Google Play app store to infect users in South and Southeast Asia with spyware capable of monitoring the target's call logs, and various others, and text messages.

April2020 - During Covid 19 pandemic an attempt to break into WHO's staff -accounts had occurred and the face behind the event was targeted upon Iranian government-support hackers.

April 2020- U.S. officials reported seeing a sudden and great increase of attacks by Chinese hackers against healthcare providers, pharmaceutical manufacturers, and the U.S. Department of Health and Human services during the time of the COVID-19 pandemic.

June 2020 - Nine human rights activists in India were targeted as part of a coordinated spyware campaign that started to use malware to log their keystrokes, record audio, and steal credentials.

August 2020- Taiwan accused Chinese hackers of infiltrating the information systems of at least ten government agencies and 6,000 email accounts to gain access to citizens' personal data and government information.

August 2020- Pakistani hackers were suspected to have used custom malware to steal files of victims in 27 countries across the globe, including India and Afghanistan.
August 2020- Military and financial organizations were targeted by Chinese Cyber espionage groups across the Eastern Europe.
August 2020- Pakistan claimed that mobile phones of their military personnel and government officials were hacked by intelligence agencies of India.
September 2020- The Universal Health Systems sustained a software designed by criminals to prevent computers users from getting access to their own that caused affected hospitals to revert to manual backups, divert ambulances, and reschedule surgeries .
September 2020- A patient had died due to ransomware attack on german hospital which made him move to a more distant hospital for his treatment.
September 2020- The Iranian hackers had exploited public known vulnerabilities so that they can target the U.S organisations in the IT,government,healthcare, finance and media sector as it was announced by the FBI and CISA.
September 2020-Georgian officials announced that COVID-19 research files at a biomedical research facility in Tiblisi was targeted as part of a cyberespionage campaign .
September 2020-Norway announced that they had defended themselves against two cyber attacks which targeted the emails of certain employees and members of the Norwegian parliament as well as public employees in the Hedmark region.
September 2020- 5 Chinese hackers in relation to chinese intelligence services were indicated by the The U.S. Department of Justice for attacks on more than 100 organizations across government, IT, social media, academia, and other sectors.
October 2020 - previously unknown cyber espionage group was found to have been stealing documents from government agencies and corporations in Eastern Europe and the Balkans since 2011.
Cybersecurity Ventures predicts that there will be 6 billion Internet users by 2022, and 7.5 Billion Internet users by 2030.[25]

INDIAN PERSPECTIVE

According to Indian scenario of cyberspace crimes and cyber space laws, there was no statute in India for governing Cyber Laws involving privacy issues, jurisdiction issues, intellectual property rights issues and a number of other legal questions. With the tendency of misusing the technology, there arises a need of strict statutory laws to regulate the criminal activities in the cyber world and to protect the true sense of technology thereby IT ACT, 2000 was enacted by Parliament of India to protect the field of e-commerce, e-governance, e-banking as well as penalties and punishments in the field of cyber crimes. The above Act was further amended in the form of IT Amendment Act, 2008. Also certain sections of IPC were also amended as per the needs of society. Both IT Act and Indian penal code are the only legal framework in India to provide protection to combat cybercrime.

[25]https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/; Cybersecurity Ventures Official Annual Cybercrime Report, 2020

IT legislation in India: Mid 90's saw an impetus in globalization and computerization, with more and more nations computerizing their governance, and e-commerce seeing enormous growth. Previously, most of international trade and transactions were done through documents being transmitted through post and by telex only. Evidence and records, until then, were predominantly paper evidence and paper records or other forms of hard-copies only. It is against this background the Government of India enacted its Information Technology Act 2000 with the objectives as follows, stated in the preface to the Act itself. "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."

In India the Information Technology Act 2000 was passed to provide legal recognition for transactions carried out by means of electronic communication. The Act deals with the law relating to Digital Contracts, Digital Property, and Digital Rights Any violation of these laws constitutes a crime. The Act prescribes very high punishments for such crimes. The Information Technology (amendment) Act, 2008(Act 10 of 2009), has further enhanced the punishments. Life imprisonment and fine upto rupees ten lakhs may be given for certain classes of cyber crimes. Compensation up to rupees five crores can be given to affected persons if damage is done to the computer, computer system or computer network by the introduction of virus, denial of services etc.

Information technology has spread throughout the world. The computer is used in each and every sector wherein cyberspace provides equal opportunities to all for economic growth and human development. As the use of cyberspace grows increasingly diverse and the range of online interaction expands, there is expansion in cyber crimes i.e. breach of online contracts, perpetration of online torts and crimes etc.

It shows the requirement of strict laws by the cyberspace authority for regulating cyber criminal activities and better judicial actions to provide justice to the victims of cyberspace. To monitor cyber crimes particularly cyber terrorism and hackers, proper regulatory bodies and law are essence of the era. Various provisions that deal with cyber crime resulting in violation of human rights are :- Penalty and Compensation for damage to computer, computer system, etc (sec. 43 IT act) , Compensation for failure to protect data (sec. 43A IT Act) , Tampering with computer source Documents (sec. 65 IT Act) , Hacking with computer systems, Data Alteration (sec. 66 IT Act) , Sending offensive messages through communication service, etc (sec. 66A IT Act) , Dishonestly receiving stolen computer resources or communication device (sec. 66B IT Act) , Identity theft (sec. 66C IT Act) , Cheating by personating by using computer resource (sec. 66D IT Act) , Violation of privacy (sec. 66E IT Act) , Cyber terrorism (sec. 66F Act) , Publishing or transmitting obscene material in electronic form (sec. 67 IT Act) , Publishing or transmitting of material containing sexually explicit act, etc. in electronic form (sec. 67A IT Act) , Punishment for publishing or transmitting of material depicting children in sexually explicit acts, etc. in electronic form (sec. 67B IT Act) , Preservation and Retention of information by intermediaries (sec.67C IT Act) , Powers to issue directions for interception or monitoring or decryption of any information through any computer resource (sec. 69 IT Act) , Power to issue directions for blocking for public access of any information through any computer resource (sec. 69A IT Act) , Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security (sec. 69B IT Act) , Un-authorized access to protected system (sec. 70 IT Act) , Penalty for misrepresentation (sec. 71 IT Act) , Breach of confidentiality and privacy (sec. 72 IT Act) , Publishing False digital signature certificates (sec. 73 IT Act) , Publication for fraudulent purpose (sec. 74 IT Act) , Act to apply for offence or contraventions committed outside India (sec. 75 IT Act) , Compensation, penalties or confiscation not to interfere with other punishment(sec. 77 IT Act) , Compounding of Offences (sec.77A IT Act) , Offences with three years imprisonment to be cognizable (sec. 77B IT Act) , Exemption from liability of intermediary in certain cases (sec. 79 IT Act) , Punishment for abetment of offences (sec. 84B IT Act) , Punishment for attempt to commit offences (sec. 84C IT Act) and Offences by Companies (sec. 85 IT Act). The applications of these sections are subject to the investigating style of investigating officer and charge sheet filed by the investigating agency and nature of cyber crime. The Information Technology Act, 2000, was thus passed as the Act No.21 of 2000, got the President's 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 , Offenses and Contraventions , Justice Dispensation Systems for cyber crimes.

Being the first legislation in the nation on technology, computers & 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. There were some conspicuous omissions too resulting in the investigators relying more and more on the time-tested (one and half century-old) Indian Penal Code even in technology based cases with the I.T. Act also being referred to in the process and the reliance more on IPC rather on the ITA. Thus the need for an amendment – a

detailed one – was felt for the I.T. Act almost from the year 2003-04 themselves. Many recommendations were observed and subsequently taken up as a comprehensive Amendment Act and after considerable administrative procedures; the consolidated amendment called the Information Technology Amendment Act 2008 was placed in the Parliament and passed without much debate, towards the end of 2008.

The Amendment Act got the President assent on 5 Feb 2009 and was made effective from 27 October 2009. Some of the notable features of the ITAA are as follows: Focusing on data privacy , Focusing on Information Security , Defining cyber café , Making digital signature technology neutral , Defining reasonable security practices to be followed by corporate , Redefining the role of intermediaries , Recognizing the role of Indian Computer , Emergency Response Team , Inclusion of some additional cyber crimes like child pornography and cyber terrorism , Authorizing an Inspector to investigate cyber offences (as against the DSP earlier) .

III. CONSTITUTIONAL LIABILTY

The Constitution being the supreme law of India has huge responsibility to protect the rights of its citizens as well as foreigners when the issue is about violation of their basic human rights. These rights are inalienable and inherent by the people across the globe. Even though these rights are a necessity for human survival, there are certain sectors which still need to synchronize accordingly. Cyberspace is one of such, since technology is pacing up with high speed the Indian legislature and regulatory bodies are still lacking behind in providing proper legal aid. Cybercrime can be done against persons, organization, government, property etc. The preamble of our constitution itself promises justice, liberty and equality to all the people. Thereby providing the right to life, right to equality, right to freedom of speech and expression and various others to ensure the dignified survival of the citizens.

Cyberspace criminals invade electronic devices of people to steal data in order to use them for their own motives. Such acts imply the violation of "right to privacy". Constitution of India does not provide right to privacy as prima facie fundamental right but imbibe in Article 21 i.e. Right to life of Indian constitution.

In Justice K.S. Puttaswamy (Retd) v. Union of India,[26] Hon'ble Supreme Court of India held that 'The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution'. Therefore, whenever there is cybercrime violation in respect of a person's private property or his personal belongings, then the accused can also be charged under Article 21 of the Indian Constitution.[27] Right to privacy is not the only right attached to article 21 of indian constitution, with the recent judgement of Faheema Shirin v. State of Kerala[28], "where the right to internet access was recognised as a fundamental right forming a part of the right to privacy and the right to education under Article 21 of the constitution"; cyberspace is becoming an integral part of human life in the modern era.

It is a fundamental right of the Individual to retain private information concerning himself under Article 21 of the Indian Constitution, which says: No person shall be deprived of his life or personal liberty except according to procedure established by law. And due to the increasing trend of the Crime rate in the field separate legislation is required in this context for better protection of individuals.[29]

Article 19 i.e. freedom of speech and expression, but the same is to be followed looking over the reasonable restriction withstanding in the clause (2) of provision stated as, in 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 offense." The Internet is the biggest platform where people express their views, debates and information. From big ventures to startups, invests in their website over the internet which provides them with customers and their opinions. . Court in the case[30], have recognised the importance of freedom of speech and expression not only from the point of view of the liberty of the individual but also from the point of view of democratic governance because public criticism is essential to the working of its institutions.

Section 66A of the IT act states the punishment for sending offensive messages through communication service i.e. via, electronic mail through computer or any other communication device like a mobile phone or a tablet. A conviction can extend to term of maximum three years in jail and fine. But in the recent judgment, Shreya Singhal v. Union of India; decided on 24th March, 2015, apex court struck down section 66A of the amended Indian information act 2000 a provision in the cyber law which provides power to arrest a

[26]Justice K.S. Puttaswamy (Retd) v. Union of India, WRIT PETITION (CIVIL) NO. 494 OF 2012

[27] https://www.lawctopus.com/academike/cyber-crimes-other-liabilities/;Crimes in Cyberspace: Right to Privacy and Other Issues, By Mohak Rana

[28]Faheema Shirin.R.K vs State Of Kerala on 19 September, 2019

[29]http://www.legalserviceindia.com/article/l146-Cyber-Crime-And-Law.html

[30]Romesh Thappar v. State of Madras (1950)SCR 594

person for posting allegedly "offensive" content on websites. The apex court ruled that the section falls outside Article 19(2) of the constitution which relates to freedom of speech, and thus has to be struck down in its entirety[31]. The court in the case relied upon, Secretary, Ministry of Information &Broadcasting v. Cricket Association of Bengal[32]and held that right to acquire and disseminate information forms part of freedom of speech and expression.

In the case of Kharak Singh v. The State of U.P., The Supreme Court for the first time recognized that citizens of India had a fundamental right to privacy which was part of the right to liberty in Article 21 as well as the right to freedom of speech and expression in Article 19(1)(a), and also of the right of movement in Article 19(1)(d).

PUCL v. Union of India[33], apex court in the case observed that right to freedom of speech and expression is guaranteed under Article 19(1)(a) of the constitution, freedom here means the right to express one's opinions freely by word of mouth, writing, printing, picture, or in any other manner.

Ranjeet D. Udeshi v. State of Maharashtra[34], the Supreme Court admitted that Indian Penal Code doesn't define obscenity though it provides punishment for publication of obscene matter. There's a very thin line existing between a material which could be called obscene and the one which is artistic. Court even stressed on the need to maintain balance between the fundamental right of freedom of speech and expression and public decency and morality. If matter is likely to deprave and corrupt those minds which are open to influence to whom the material is likely to fall. Where both obscenity and artistic matter is so mixed up that obscenity falls into shadow as its insignificant then obscenity may be overlooked.

With the struck down of section 66A of IT Act, judiciary made it clear that the freedom of speech and expression is important for the beings and the same should not be violated. It is the cornerstone for any democracy as well liberty for an individual. But by giving the importance to the citizens rights does not give them the right to violate others reputation or their fundamental rights. It is important for them to keep in mind that democracy never gives absolute rights and liberties to its citizens rather duties along with it. Freedom of speech and expression should be exercised in a way that the same shall not come under the umbrella of defamation, obscenity, illegality, sedition, offensive remarks or violate others' privacy. With the advancement of technology the internet has become a platform for inter- personal or business conversations even for third world countries like India. Diversified opinions, comments, ideas, beliefs, judgments, critics are required for the proper analysis of information. Art-19 (1)(a) of Indian constitution, 1950 provides the freedom of speech and expression, Article 19 of Universal Declaration of Human Rights, 1948 and Article 19 (2) of International Covenant on Civil and Political Rights, 1966 imparts that everyone shall have the right to freedom of expression and the right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

In Kerala Voluntary Health Services v. Union of India, Kerala High Court observed that apart from the reasonable restrictions enumerated in Art.19(2), the freedom of speech and expression guaranteed by Art.19(1)(a) is also circumscribed by the right to life guaranteed under Art.21 of the Constitution. The malicious comments and remarks directed at a person tears away his most valued asset in the form of reputation and invades into his right to privacy. Both right to reputation and privacy are facets of right to life under Art. 21.[35]

The cyber explosion was not contemplated by the framers of our Constitution when Art. 19 (2) was inserted. The ill effects of misuse cyber speech were not in their minds and so it is for the Parliament to suitably amend Art. 19 (2) so as to contain in its ambit restriction on misuse of cyber free speech. [36]

IV. CRIMINAL LIABILITY

Criminal liability in India for cyber crimes is defined under the Indian Penal Code (IPC). Certain sections of IPC that deal with the various cyber crimes are as follows: Sending threatening messages by email (Sec .503 IPC); Word, gesture or act intended to insult the modesty of a woman (Sec.509 IPC); Sending defamatory messages by email (Sec.499 IPC); Bogus websites , Cyber Frauds (Sec .420 IPC); E-mail Spoofing

[31] https://www.lexology.com/library/detail.aspx?g=8ca29f1a-6e00-45ab-ad8f-ee6ff3ab6161; Shreya Singhal v. Union of India,WRIT PETITION (CRIMINAL) NO.167 OF 2012

[32]Secretary, Ministry of Information & Broadcasting v. Cricket Association of Bengal, AIR 1995 SC 1236

[33]PUCL v. Union of India , AIR 1997 SC 568

[34]Ranjeet D. Udeshi v. State of Maharashtra,1965 AIR 881; http://www.legalserviceindia.com/article/l146-Cyber-Crime-And-Law.html

[35]file:///C:/Users/chirag/Documents/2-6-185-421.pdf; WP(C).No. 38513 of 2010 (S)

[36]file:///C:/Users/chirag/Documents/2-6-185-421.pdf; Misuse of free speech in cyber world and conflicting rights byBarla Mallesh Yadav

(Sec .463 IPC); Making a false document (Sec.464 IPC); Forgery for purpose of cheating (Sec.468 IPC); Forgery for purpose of harming reputation (Sec.469 IPC); Web-Jacking (Sec. 383 IPC); E-mail Abuse (Sec .500 IPC); Punishment for criminal intimidation (Sec.506 IPC); Criminal intimidation by an anonymous communication (Sec.507 IPC); Obscenity (Sec. 292 IPC); Printing etc. of grossly indecent or scurrilous matter or matter intended for blackmail (Sec.292A IPC); Sale, etc., of obscene objects to young person (Sec .293 IPC); Obscene acts and songs (Sec.294 IPC); Theft of Computer Hardware (Sec. 378); Punishment for theft (Sec.379). Other then the IPC some other piece of legislations also imposes criminal liability on the accused and these legislations are:- Online Sale of Drugs (NDPS Act); Online Sale of Arms (Arms Act) ;Copyright infringement (Sec.51 of copyright act, 1957); Any person who knowingly infringes or abets the infringement of (Sec.63 of copyright act, 1957); Enhanced penalty on second and subsequent convictions (Sec.63 A of copyright act, 1957) and Knowing use of infringing copy of computer program to be an offence (Sec.63B of copyright act, 1957). In India there are a number of cases filed under these IPC provisions related to cyber crime. According to the report of the Home Ministry, in 2012 there were 601 cases filed under the various provisions of IPC.[37]

V. CYBER CRIME CASES IN INDIA

State of Tamil Nadu v. Suhas Katti[38];The case related to posting obscene, defamatory and annoying messages about a divorced 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. This is considered as the first case in the state of Tamil Nadu, in which the offender was convicted under section 67 of Information Technology Act 2000 in India.

Syed Asifuddin and Ors. v. The State of Andhra Pradesh[39]; In this case, Tata Indicom employees who manipulated the electronic 32- bit number (ESN) programmed into cell phone theft were exclusively franchised to Reliance Infocomm. Court held that tampering with source code invokes Section 65 of the Information Technology Act.

Sony.Sambandh.Com Case[40];A complaint was filed by Sony India Private Ltd, which runs a website called www.sony sambandh.com, targeting Non Resident Indians. In May 2002, someone logged onto the website under the identity of Barbara Campa and ordered a Sony Colour Television set and a cordless headphone. She gave her credit card number for payment and requested that the products be delivered to Arif Azim in Noida. After one and a half months the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase. The company lodged a complaint for online cheating at the Central Bureau of Investigation. The court convicted Arif Azim for cheating under Section 418, 419 and 420 of the Indian Penal Code. This was the first time that a cyber crime has been convicted. The judgment is of immense significance for the entire nation. Besides being the first conviction in a cyber crime matter, it has shown that the Indian Penal Code can be effectively applied to certain categories of cyber crimes which are not covered under the Information Technology Act 2000.

S. Sekar v The Principal General Manager (Telecom) (B.S.N.L.)[41];The petitioner is an employee of the second respondent, B.S.N.L, working as a Telecom Technical Assistant (Switch). It so happened that while he was working in SIPCOT MBM Main Exchange, Keeranur, the B.S.N.L. higher officials suspected him and others for having committed offences in manipulating the computer system and thereby causing loss to B.S.N.L. The FIR in Crime No. 1 of 2004 was registered on 06.01.2004 by the Police, Pudukottai, for the offences under Section 406, 420 and 468 I.P.C. and 43(g) of the Information Technology Act, 2000. The main thrust of the grievance of the petitioner in this case is that when there is a special enactment namely, the Information Technology Act, 2000, which is in operation relating to the alleged misconduct attributed as against the petitioner, there is no question of invoking the penal sections under the Indian Penal Code, It was held that the Police to investigate thoroughly into the matter and add or delete the penal Sections under the Information Technology Act, 2000, as well as IPC and ultimately, it is for the criminal court which would seize the matter to

[37]http://www.mha.nic.in accessed on 4th Dec 2013
[38]State of Tamil Nadu Vs Suhas Katti, 4680 of 2004 Criminal Complaint
[39]Syed Asifuddin and Ors. Vs. The State of Andhra Pradesh, 2006 (1) ALD Cri 96, 2005 CriLJ 4314
[40]Sony.Sambandh.Com Case, 2013
[41]S. Sekar v The Principal General Manager (Telecom) (B.S.N.L.), W.P. (MD) No.10208 of 2005 and M.P.No.10905 of 2005

decide on that. The Section 43(g) of the Information Technology Act, 2000, invoked by the police and specified in the FIR is declared void. Accordingly, the Writ petition is ordered. No costs, connected M.P. is closed.

Andhra Pradesh Tax Case[42]; Dubious tactics of a prominent businessman, from Andhra Pradesh, were exposed after officials of the department got hold of computers, used by the accused in one of the many cyber fraud cases in India. The owner of a plastics firm was arrested and Rs 22 crore cash was recovered from his house by sleuths of the Vigilance Department. They sought an explanation from him regarding the unaccounted cash within 10 days. The accused submitted 6,000 vouchers, to prove the legitimacy of trade and thought his offence would go undetected but after careful scrutiny of vouchers and contents of his computers, it was revealed that all of them were made after the raids were conducted. It was later revealed that the accused was running five businesses under the guise of one company and used fake and computerised vouchers to show sales records and save tax.

SMC Pneumatics (India) Pvt. Ltd. vs. Jogesh Kwatra[43];In India's first case of cyber defamation, the High Court of Delhi assumed jurisdiction over a matter where a corporation's reputation was being defamed through emails and passed an important ex-parte injunction. In this case Delhi High Court assumes tremendous significance as this is the first time that an Indian Court assumes jurisdiction in a matter concerning cyber defamation and grants an ex-parte injunction restraining the defendant from defaming the plaintiff by sending derogatory, defamatory, abusive and obscene emails either to the plaintiffs or their subsidiaries.

Cyber Attack on Cosmos Bank[44];In August 2018, the Pune branch of Cosmos bank was drained of Rs 94 crores, in an extremely bold cyber attack. By hacking into the main server, the thieves were able to transfer the money to a bank in Hong Kong. Along with this, the hackers made their way into the ATM server, to gain details of various VISA and Rupay debit cards. The switching system i.e. the link between the centralized system and the payment gateway was attacked, meaning neither the bank nor the account holders caught wind of the money being transferred. According to the cybercrime case study internationally, a total of 14,000 transactions were carried out, spanning across 28 countries using 450 cards. Nationally, 2,800 transactions using 400 cards were carried out. This was one of its kinds, and in fact, the first malware attack that stopped all communication between the bank and the payment gateway.

Bomb Hoax Mail Case[45];In an email hoax, sent by a 15-year-old boy from Bangalore, the Cyber Crime Investigation Cell (CCIC) arrested him in 2009. The boy was accused of sending an email to a private news company saying, "I have planted 5 bombs in Mumbai, you have two hours to find them". The concerned authorities were contacted immediately, in relation to the cyber case in India, who traced the IP address (Internet Protocol) to Bangalore.

Bazee.com case[46];The CEO of Bazee.com was arrested in December 2004 because a CD with objectionable material was being sold on the website. The CD was also being sold in the markets in Delhi. The Mumbai Police and the Delhi Police got into action. The CEO was later released on bail. This opened up the question as to what kind of distinction we draw between Internet Service Provider and Content Provider. The burden rests on the accused that he was the Service . Provider and not the Content Provider. It also raises a lot of issues regarding how the police should handle cybercrime case

VI. CYBER CRIMES AGAINST WOMEN AND CHILDREN

Cyber crimes against women and children are on the raise and they have been drastically victimized in cyberspace. There are some people who try to defame women and children by sending obscene emails, stalking women and children by using chat rooms, websites etc, developing pornographic videos where women and children are depicted in compromising positions mostly created without their consent, spoofing emails, morphing of images for pornographic content etc. Massive awareness needs to be created among women and children regarding the safe use of Mobile Phones, Computers and the Internet.

Women and children have been found to be most easily deceived in the online world with cyber crimes against women and children witnessing a sharp rise over the last couple of years. Women are often subjected to cyber crimes such as cyber harassment, online stalking, cyber pornography, cyber defamation, matrimonial frauds and much more.

Children are soft targets for cyber criminals as most of the teenagers and adolescents have their online presence without adult guidance. It is hard to get over the spate of deaths of innocent teenagers resulting from

[42]Andhra Pradesh Tax Case judgement on April 23, 1987
[43]SMC Pneumatics (India) Pvt. Ltd. vs. Jogesh Kwatra decided on 12 February, 2014
[44]Cyber Attack on Cosmos Bank decided on August 2018
[45]Bomb Hoax Mail decided on April 23, 1982
[46]Bazee.com case ,2008;105 DRJ 72

the online suicidal game – Blue Whale. In fact, as parents, if you observe restlessness, insomnia, excess addiction to the internet or other unnatural changes in your child's behavior, then it is about time that you exercise caution and monitor your child's online activities .

Apart from these, online monetary fraud has also become a daily news. Each day, thousands of innocent individuals fall prey to online banking and credit/debit card frauds. Statistics show that over 25,800 online banking frauds were reported in 2017, amounting to nearly □179 crore which is surely a huge amount .

The National Cyber Safety and Security Standards is going to introduce a Cyber Awareness Program (CAP) for Women & Children designed specifically for the safety of women & children. The CAP will focus on very sensitive issues towards the cyber safety of women and children. This program will encourage women & children to adopt safe computing skills and it will promote good security practice. CAP will aim to make women & children aware not only of the risks they face in CyberSpace, but also of the counter measures they can utilize to protect themselves. By implementing this type of programs, we can allow our children to reap the full benefits of the Internet and have a safer online experience.

Women and children are the most vulnerable beings, and having no security or legislation against such crime makes them an easy target. Sexual harassment, stalking, life threatening games, morphing of images, illegal websites, dark net, pornography, obscene videos of children, abusive content and impersonation by criminals affect their right to privacy, health, dignity and life, often leaving a dark scar on their Psychology and physical existence . This shows how cyberspace has its strings attached to the real world. Women and children should be made aware of various cyber crimes over the internet and how to report and deal in an effective manner. There must be an active participation in relation to reduction of these crimes.

VII. CONCLUSION

Though not all people are victims of cyber crimes , they are still at risk. Usage of the internet is no more a luxury but a fundamental right as per Indian Judiciary. Crimes done behind the computer screen are the 21st century's problem . With the increase in technology the work of cyber criminals are getting easier, due to lack of synchronization between legislation and pace of technology. All sorts of data, whether it is personal or governmental, need high security. It is predicted in a report that by 2021 cybercrime will affect information worth $6 trillion. A netizen should take certain precautions while operating the internet. The Internet could be bliss as well a boon depending upon the usage. With the internet becoming an integral part of daily life it is important to understand the consequences and the drastic impact it can cause to fellow beings. A scheme for the establishment of Indian Cyber Crime Coordination Centre has been established to handle issues related to cybercrime in the country in a comprehensive and coordinated manner. As Cyber Crime is a major threat to all the countries worldwide, certain steps should be taken at the international level to prevent cybercrime. Complete justice must be provided to the victims of cyber crimes by way of compensatory remedy and strict actions against the offenders in order to set an example so that it will anticipate the criminals of cyber crime. The IT department should pass certain guidelines and notifications for the protection of computer systems and it should also bring out some strict laws to break down the criminal activities relating to cyberspace. It is the responsibility of web site owners to adopt policy against cybercrime as the number of internet users are growing day by day . It is better to use a security programme to control information and movement on sites. Online cybercrime reporting portal has been launched to report complaints pertaining to Child Pornography/Child Sexual Abuse Material, rape/gang rape imageries or sexually explicit content. Safeguards are needed to ensure that laws place restrictions on Internet access, abuse of content and privacy matters in accordance with rule of law and human rights. An internationally acceptable law should be there to safeguard the human rights of individuals in cyberspace . To protect the human rights of individuals in cyberspace international organisations must prepare effective and efficient laws which can deal with the cyber crimes that affect the human dignity of the individuals and also the human rights of expression. It's a pronged process for the law making authorities to stop such activities which violate the human rights of the individuals. In the recent years we can see that in the UN Human Rights Council's 17th Session, the UNO considered Internet access a Human Right and disconnecting or limiting the people from expressing their views on the internet , a violation of Human Rights[47]. Providing human rights to citizens does not mean absolute freedom instead reasonable actions. With rights comes duties and liabilities. Article 19 provides freedom of speech and expression, Article 21 provides right to life with dignity, with a healthy body but they come with restrictions. Rule of law clearly states no one is above law and the same shall be kept in mind while exercising them.

[47]https://en.wikipedia.org/wiki/Human_rights_in_cyberspace