IMPACT: International Journal of Research in Humanities, Arts and Literature (IMPACT: IJRHAL)
ISSN (P): 2347-4564; ISSN (E): 2321-8878
Vol. 6, Issue 7, Jul 2018, 403-420

CYBER CRIME, ISSUES AND CHALLENGES TO INDIAN LEGAL SECURITY SYSTEM

Madhu Bala

Assistant Professor, Department of Laws, Guru Nanak Dev University, Regional Campus, Gurdaspur, Punjab, India

Received: 15 Jul 2018 **Accepted:** 20 Jul 2018 **Published:** 31 Jul 2018

ABSTRACT

Crime cannot be defined in definite words. It erupts in various forms within society. As far as cyber crime is concerned, it has taken a dangerous form which is a constant threat to the whole world. The technology is developing by leaps and bound. It has a more negative impact on whole society. With the development of technology cybercriminals more easily commit crimes at cyberspace. Cyber frauds, hacking, phishing, cyber terrorism, cyber pornography especially child porn pornography, cybertrespass against the intellectual properties, cyber defamation and cyberstalking are some of the serious crimes which are being committed on cyberspace. It causes financial and physical damage to the concerned individuals and to the government also. The women are soft target of the cyberstalkers. These criminals upload the obscene pictures of women and send them vulgar comments by hacking the social accounts of the females. In India, The Information Technology Act, 2000 is a law against the cybercrimes. This Act was amended in 2008 and inserted new terms like cyber terrorism, cyberstalking. The new amended The Information Technology Act, 2008 also enhances the punishments and fines in order to curb the menace of cyber crime. Besides, Indian Penal Code, 1860 also contains the relevant provisions to punish the cybercriminals. Both these laws can concurrently punish the cybercriminals. Hence, laws cannot be implemented adequately unless the people get knowledge of these laws. They should have to be conscious about these laws in order to prevent the cyber crimes. In India, lack of knowledge and ignorance on the part of the people is one of the biggest hindrances to prevent the cyber crimes. There is a need to impart knowledge to people that how and where to file complaints against cybercrimes. Besides, cyber cell authorities should also take immediate action against the cyber criminals which would have a deterrent effect on other culprits.

KEYWORDS: *Cyber-Stalking, Dissemination of Obscene Material Defamation, Hacking, Phishing, Cyber Pornography, Crimes against Persons Property, Cyber Terrorism, Child Pornography*

INTRODUCTION

Cybercrimes are the most unpredictable calamity in the cyber world. Unauthorized access, hacking, spreading of viruses, smashing computer networks on a very large scale, the brutal weapons like e-mail bombing, logic bombs resulting into the disrupt behavior of computer networks are very few incidences of recent days. The very same virtues of the internet when gone in wrong hands or when exploited by people with dirty minds and malicious intentions can make it a virtual hell. As a result of the rapid adoption of the internet globally, cybercrimes include not only hacking and cracking but also extortion, child pornography, money laundering, cyberstalking, fraud, software pirating and corporate espionage to name a few. Law enforcement officials have been

frustrated by the inability of legislators to keep cybercrimes legislation at par with of the fast-moving technology.[1]

Cybercrime is an evil having its origin in the growing dependence on computers in modern life. In a day and age when everything from microwave ovens and refrigerators to nuclear power plants is being run on computers, cybercrime has assumed rather sinister implications. The computer crime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to IPC. The abuse of computers has also given birth to the gamut of new age crimes that are addressed by the Information Technology Act, 2000. The Information Technology Act, does not define cybercrime but specifies many acts as an offense and makes them punishable in certain circumstances. But it would be unsuitable to restrict to all crimes describes under the Information Technology Act as IPC, Copyrights Act and Patent Act also cover many forms of cyber crimes.[2]

ORIGIN OF CYBER CRIME

When the internet was developed, the founding fathers of the internet hardly had any inclination that the internet could transform itself into an all-pervading revolution which could be misused for criminal activities and which required regulation. Today, there are many disturbing things happening in cyberspace. Due to the anonymous nature of the internet, it is possible to engage in a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the internet to perpetuate criminal activities in cyberspace. The first recorded cyber crime took place in the year 1820. That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500BC in India, japan China. The era of modern computers, however, began with the analytical engine of Charles Babbage. In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage jacquard from further use of the new technology. This is the first recorded cybercrime.[3]

TYPES OF CYBER CRIMES

Nowadays, Cyber crimes have become a major threat with its new forms for the whole world due to the fastest development of the technology. It is noticed that various cyber crimes have been flooded on internet. Therefore, division of cyber crimes in India have been made under following categories:-

Cyber Crimes against Persons[4]

Cyber-Stalking

It is a crime to stalk someone on the internet by using technology. CyberStalking can be done by using the internet, sending e-mails, by using the phone to call unknown persons, through webcam and videos etc. It has become easy to stalk on social sites due to easy accessibilities of phones and to get mobile data on cheap prices. Now people are less interested to use computers as they do not want to stick at one place. On the other hand, people are more interested to use

mobile phones in order to explore the social sites.[5] Generally, stalking can be termed as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, killing the victim's pet, vandalizing victims property, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harm to the victim. CyberStalking means repeated acts of harassment or threatening behavior of the cybercriminal towards the victim by using internet services. Both kinds of Stalkers i.e. Online & Offline have the desire to control the victim's life.[6] The Information Technology Act, 2000 did not recognize the term but due to Ritu Kohli's case, the amended Act of 2008 recognized Cyber Stalking. In a case, in 2003, Seema Khanna (name changed), an employee with an embassy in New Delhi, know that web surfing would lead to an invasion of her privacy. In an apparent case of cyberstalking, Khanna (32) received a series of e-mails from a man asking her to either pose in nude for him or pay Rs 1 lakh to him. She filed a complaint to Delhi Police and asserted that she started receiving these mails in the third week of November. The accused threatened Khanna that he would put her morphed pictures on display at sex websites, along with her telephone number and address. The accused mailed the woman her photographs. The woman claimed these were the same photographs which she had kept in her mail folder. The police said the accused had hacked her e-mail password which enabled him to access the pictures. A preliminary inquiry into the complaint has revealed that the emails were sent to the victim from a cyber cafe in south Delhi. The police felt that the accused might be known to the victim as he seemed to know a lot about her. The cyberstalker can be booked under Section 509 of the IPC for outraging the modesty of a woman and also under the Information Technology Act, 2000. But the police admitted that IT Act, 2000 was not enough to deal with cyberstalking.[7]

Ritu Kohli's case is the first case in India dealing with cyberstalking. The Delhi Police arrested Manish Kathuria the culprit of the case. In the said case, Manish was stalking a person called Ritu Kohli on the Net by illegally chatting on the website www.mirc.com with the name of Ritu Kohli. Manish was regularly chatting under the identity of Ritu Kohli on the said Website, using obscene and obnoxious language, was distributing her residence telephone number and inviting chatter to chat with her on the telephone. Consequently, Ritu Kohli was getting obscene calls from different chatters from various parts of India and abroad. Ritu Kohli reported the matter to the police and the Delhi Police swung into action. The police had registered the case under Section 509 of the Indian Penal Code, 1860 for outraging the modesty of Ritu Kohli. But Section 509 of the Indian Penal Code, 1860 only refers to a word, gesture or act intended to insult modesty of a woman. But when some things are done on the internet, then there is no mention about it in the said section. None of the conditions mentioned in the section cover cyberstalking. Ritu Kolhi's case was an alarm to the Government, to make laws regarding the aforesaid crime and regarding the protection of victims under the same. As a result Section 66A of The Information Technology (Amendment) Act, 2008 was added[8]

Section 354 D of the Indian Penal Code, 1860 provides that whoever commits the offence of stalking shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and shall also be liable to fine and be punished on a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years and shall also be liable to fine.[9]

Section 66D of The Information Technology (Amendment) Act, 2008 prescribes punishment for cheating by personation by using computer resource that whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees. Section 66E of The Information Technology (Amendment) Act, 2008 provides punishment for violation of privacy that whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees rupees or with both.

Dissemination of Obscene Material: It includes Indecent exposure/ Pornography (basically child pornography), hosting of the web site containing these prohibited materials. These obscene matters may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind. In 2016, the former President's Dr. Pranab Mukhjree's daughter Sharmistha received the obscene comments on facebook wall from the unknown person. Instead of blocking that person she filed a complaint in Delhi Police Cyber Cell. Later, I was found that man named Partha Mandal belonged to West Bengal and he did not know anything about her. Later, He apologized to her.[10]

Defamation: It is an act of imputing any person with intent to lower down the dignity of the person by hacking his mail account and sending someemails with using vulgar language to the unknown persons mail account. Section 500 of The Indian Penal Code, 1860 provides punishment for defamation that whoever defames another shall be punished with simple imprisonment for a term which may extend to two years or with fine or with both.[11]

Further, Section 509 of The Indian Penal Code, 1860 provides that whoever, intending to insult the modesty of any woman, utters any word, makes any sound or gesture or exhibits any object, intending that such word or sound shall be heard, of that such gesture or object shall be seen, by such woman or intrudes upon the privacy of such woman, shall be punished with simple imprisonment for a term which may extend to one year or with fine or with both.[12]

On the other hand, Section 67 of The Information Technology (Amendment) Act, 2008 contains punishment for publishing or transmitting obscene material in electronic form. Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to two-three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five

years and also with fine which may extend to ten lakh rupees.[13]

Section 67A of The Information Technology (Amendment) Act, 2008 prescribes punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.[14]

IDENTITY THEFT AND DATA THEFT

Identity means recognition and theft means to steal. It means to steal someone's private information through different means. Identity theft means to steal the personal information of any person with the purpose to extort illegal money. Data theft itself includes the identity theft. A person steals the personal information of another individual with the intention to commit other crimes and to grab illegal money. According to government records, the identity of an individual can be described by birth registration, voter card, driving licenses, pan cards and aadhar cards etc.[15]

These documents contain all the relevant information regarding each person. In these documents, the name, age, address, citizenship, particular mark on skin, photograph and blood group are mentioned in order to recognize that person. This is helpful for the authorities to keep a watch on persons visiting and residing within and outside country.[16] The concept of property has undergone a metamorphosis in the past decades and data is regarded as a vital property. In our daily life, we furnish a lot of personal and professional data to many entities and institutions. This data may also have enormous future value for other entities and institutions and therefore, data theft has become a serious problem for entities which hold a large amount of data. Also, a lot of data can also be stored in flash drives, CDs, micro chips, etc. making it very vulnerable against theft.[17]

On April 02, 2018 Cambridge Analytica and Facebook came under fire after the British firm was accused of harvesting personal information of over 50 million Facebook users illegally to influence polls in several countries. The IT Ministry shot off notices to both Cambridge Analytica and Facebook on the data breach issue, giving them time till March 31, 2018 and April 7, 2018,respectively, to respond. Ministry of Electronics & Information Technology, Government of India, has issued a notice to Cambridge Analytica, wherein the serious breach of propriety and misuse of data intended to profile and influence voting behavior has been highlighted. Law and IT Minister Ravi Shankar Prasad has already warned the social media giant of stringent action for any attempt to influence polls through data theft and had even threatened to summon its CEO Mark Zuckerberg, if needed.

Section 66C of The Information Technology (Amendment) Act, 2008 prescribes punishment for identity theft. According to this Section whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.[18]

Hacking: To use some ones's computer without his permission with the intention to destroy entire data saved in the computer is called hacking. Hackers can destroy whole computer programmes by sending viruses or by operating another's computer even from distant areas. Computers and mobiles are easy targets for hackers.[19] Hacking means unauthorized access to computers. Those individuals engaged in hacking activities have been termed hackers. Hacking may amount to breaking the security system of a website or a computer without the owner's permission or even knowledge, defacing it, denying services to the users of the website, changing the database or even going to the extent of damaging the system by using programmes. Similarly, the creation dissemination of harmful computer programmes which cause irreparable damage to computer systems is other kinds of cybercrime.[20]

Different Kinds of Hackers[21]

- A black hat hacker is a person who is intimately familiar with the internal details of security systems and can delve into obscure machine code when needed to find a solution to a tricky problem.
- The term white hat hacker is also often used to describe those who attempt to break into systems or networks in order to help the owners of the system by making them aware of security flaws or to perform some other altruistic activity. Many such people are employed by computer security companies and these professionals called sneakers.
- A grey hat hacker in the computer security community refers to a skilled hacker who sometimes acts legally, sometimes in good will and sometimes not.

A recent case in which two students from Kashmir named Adil Hussain and Shahid Malia were arrested by a special team of Delhi's Cyber Crime Cell on April 27, 2018. DCP Anyesh Roy, Delhi Cyber Cell claimed that both the culprits hacked 500 sites, including government sites, one of them of the Jammu and Kashmir Bank. They were also posting anti-national content on the social media and elsewhere on the web.[22]

RANSOMWARE

Ransom means to receive money in return for something. Hence, ransomware describes an encryption key which hacker keeps it in his server The purposes of the hacker to send ransomware into another's computer in order to convert the whole data into a code by using public key the encryption. The hacker or attacker of ransomware compels the victim that if he wants to get encryption key then he has to pay huge money. Hence, helpless victims fulfill the demands of the hackers.[23]

The Information and Broadcasting Minister (India) in UPA II, Kapil Sibal's personal website was hacked by Anonymous India in 2012. Interestingly, Sibal and his IT engineers learnt about it after the news had already become one of the top trends on Twitter. His website remained down continuously for many hours before it was restored to normal. The group was protesting against curbs on free speech and internet censorship which his government had decided to implement on social.[24]

Section 66 of The Information Technology (Amendment) Act, 2008 deals with computer-related offenses. This section deals with computer hacking. If any person, dishonestlyor fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.[25] Section 65 of The IT (Amendment) Act, 2008 prescribes punishment for tampering with Computer Source Documents. This Section provides that whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years or with fine which may extend up to two lakh rupees or with both.

Phishing: In this type of crimes or fraud the attackers tries to gain information such as login information or account's information by masquerading as a reputable individual or entity in various communication channels or in an email.[26] It is an act of attempting to trick customers into disclosing their personal security information, their credit card numbers, bank account details or other sensitive information by masquerading as trustworthy businesses in an e-mail. Their messages may ask the recipients to update, validate or confirm their account information. Phishing is a two-time scam, first steals a company's identity and then use it to victimize consumers by stealing their credit identities. The term Phishing (also called spoofing) comes from the fact that Internet scammers are using increasingly sophisticated lures as they fish for user's financial information and password data.[27]

In January 2013, a well-organized, sophisticated computer spy operation dubbed Red October was found to (still) be targeting high profile diplomats, governments and nuclear and energy research companies. The Red October operation used phishing emails purporting to be from companie's HR departments. The attacked covered 69 countries.[28]

In December 2013, a man was arrested for his part in a phishing scam targeting UK college students. The scam sent emails inviting students to update their student loan details on a malicious site that took large amounts of money from their accounts.[29]

Section 379 of Indian Penal Code, 1860 provides that whoever commits theft shall be punished with imprisonment of either description for a term which may extend to three years,or with fine,or with both.[30] Section 406 deals with punishment for criminal breach of trust. Whoever commits criminal breach of trust shall be punished with imprisonment of either description for a term which may extend to three years or with fine or with both.[31]

Section 43A of The Information Technology (Amendment) Act, 2008, deals with compensation for failure to protect data. When a body corporate is in possession, handling or dealing in sensitive personal data or information in a computer resource that it owns, controls or operates, is found negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or gain to any person, then in such a case the body corporate will be held liable to damages as compensation to a sum not exceeding Rs 5 Crores to the person so effected.[32] Section 66 deals with Computer Related Offences If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or withboth.[33]

Cheating & Fraud[34]: It means the person who is doing the act of cybercrime i.e. stealing password and data storage has done it with having a guilty mind which leads to fraud and cheating. It means false ATM cards i.e. Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victim's bank account mala-fidely. There is always the unauthorized use of ATM cards in this type of cyber crimes.

Section 415 of Indian Penal Code, 1860 contains the ingredients of cheating.[35] Section 417 of Indian Penal Code, 1860 provides punishment for cheating. According to this Section whoever cheats shall be punished with imprisonment of either description for a term which may extend to one year,or with fine or with both.[36]

Cyber Pornography: It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children.[37] Cyber pornography is in simple words defined as the act of using cyberspace to create, display, distribute, importor publish pornography or obscene materials. With the advent of cyberspace, traditional pornographic content has now been largely replaced by online/digital pornographic content. The Information technology has made it easier to create and distribute pornographic materials through the internet; such as material can be transmitted all over the world in a matter of seconds, the geographical restrictions which prevented to a certain extent, foreign publication to enter local territories have disappeared. The term obscene means relating to materials that can be regulated or criminalized because of their depiction of nudity, sex or excretion is patently offensive and without artistic or scientific value.[38] Freedom of speech and expression is recognized as fundamental right subject to reasonable restriction to maintain law and order, public health morality, decency etc. in Indian Constitution. However, freedom of speech and expression is restricted by section 292 and 499 of Indian Penal Code 1860. In the first case of this kind, the Delhi Police Cyber Crime

Cell registered a case under Section 67 of the Information Technology Act, 2000. A student of the Air Force Bal Bharti School, New Delhi, was teased by all his classmates for having a pockmarked face. He decided to get back at his tormentors. He created a website at the URL www.amazing-gents.8m.net. The website was hosted by him on free web space. It was dedicated to Air Force Bal Bharti School and contained text material. On this site, lucid, explicit, sexual details were given about various sexy girls and teachers of the school. Girls and teachers were also classified on the basis of their physical attributes and perceived sexual preferences. The website also became an adult boys' joke amongst students. This continued for some time till one day, one of the boys told a girl, featured on the site, about it. The father of the girl, being an Air Force officer, registered a case under section 67 of the IT Act, 2000 with the Delhi Police Cyber Crime Cell to an offense.[39]

Crimes against Persons Property[40]:

As there is rapid growth in the international trade where businesses and consumers are increasingly using computers to create, transmit and to store information in the electronic form instead of traditional paper documents. There are certain offenses which affects a person's property which is as follows **Cyber Trespass[41]:** It means to access someone's computer without the right authorization of the owner and does not disturb, alter, misuseor damage data or system by using a wireless internet connection.

Intellectual Property Crimes[42]: Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offense. The common form of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.

Cyber Squatting[43]: It means where two persons claim for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously. For example two similar names i.e. www.yahoo.com and www.yaahoo.com.

Cyber Vandalism[44]: Vandalism means deliberately destroying or damaging property of another. Thus cyber vandalism means destroying or damaging the data when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer.

Transmitting Virus[45]: Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worm attacks play major role in affecting the computerized system of the individuals.

Internet Time Thefts[46]**:** Basically, Internet time theft comes under hacking. It is the use by an unauthorized person, of the Internet hours paid for by another person. The person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge. You can identify time theft if your Internet time has to be recharged often, despite infrequent usage.

Section 441 of the Indian Penal Code contains Criminal Trespass.[47] Section 447 of Indian Penal Code, 1860 provides punishment for criminal trespass that whoever commits criminal trespass shall be punished with imprisonment of either description for a term which may extend to three months, with fine or which may extend to five hundred rupees or with both.[48]

Section 66A of The Information Technology (Amendment) Act, 2008 provides punishment for sending offensive messages through communication service, etc. and whosoever commits this offence shall be punishable with imprisonment for a term which may extend to three years and with fine.[49]

Cybercrimes against Government[50]

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

Cyber Terrorism[51]

Cyber terrorism is a major burning issue in the domestic as well as global concern. The common form of these terrorist attacks on the Internet is by the distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks etc. Cyber terrorism activities endanger the sovereignty and integrity of the nation.

Indian Parliament attack is one of the deadliest attacks on Indian Democracy. It is a case of cyber terrorism where accused committed cyber forgery and made passes, downloaded official logo, and layout map of the parliament has been downloaded through the Pakistan service provider. They controlled the e-mail and identity system of Indian Army.[52] In March 2016 the Indian Infrastructure was attacked by the Terror outfit with the name of Al Qaeda who, allegedly hacked a microsite of the Rail net page of the Indian Railways to show its sinister reach for the first time. The hacked page of Bhusawal division of Personnel Department of the Central Railway and part of a large intranet created for the department's administrative needs was replaced by a message of Maulana Aasim Umar, Al Qaeda chief in South Asia, for all Indian Muslims to participate in Jihad.[53]

Section 66F of The Information Technology (Amendment) Act, 2008 provides punishment against cyber terrorism.[54]

Cyber Warfare[55]

It refers to politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare although this analogy is controversial for both its accuracy and its political motivation. The distribution of pirated software from one computer to another with the intention to destroy the data and official records of the government.

Cybercrimes against Society at Large[56]

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

Child Pornography[57]

It involves the use of computer networks to create, distribute, or access materials that sexually exploit underage children. It also includes activities concerning indecent exposure and obscenity. Section 67 B of The Information Technology (Amendment) Act, 2008 prescribes punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.[58]

Cyber Trafficking[59]

It may be trafficking in drugs, human beings, arms weapons etc. which affects a large number of persons. Trafficking in the cyberspace is also the gravest crime.

Online Gambling[60]: Online fraud and cheating are one of the most lucrative businesses that are growing today in the cyberspace. There are many cases that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc.

Financial Crimes[61]

This type of offense is common as there is rapid growth in the users of networking sites and phone networking where culprit will try to attack by sending bogus emails or messages through the internet. Ex: Using credit cards by obtaining password illegally.

.

In order to prevent the above mentioned cyber crimes Section 45 of The Information Technology (Amendment) Act, 2008 provides for residuary penalty that whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty five thousand rupees.[62]

CONCLUSIONS

The fastest growing internet services are the result of modern needs. It is the appreciable step of inventors of fastest technology that they have made a life of the people very easy. Now, anyone can search quickly whatever comes into their mind. We can make video calling to our distant loved ones in every corner of the world. This is a very unique gift which should be used in a reasonable and fair manner but, unfortunately some miscreants misuse the technology and create troubles for others. Hackers steal all the confidential and relevant information from other's computers and commit frauds with innocent people. It becomes more challenging and troublesome for the government in case hacking of government sites which cause a threat to the peace and security of a nation. Besides, the misuse of technology intrudes on the privacy of the people. At present, women are becoming a soft target of the cyber stalkers at internet and face harassments at their hands. If the victim of cyber crime is aware of laws against cyber crimes then he/she can take action under those laws. Therefore in India The Information Technology Act, 2000 was enacted in order to prevent the cybercrimes by punishing the cyber criminals. This Act, 2000 was amended in 2008 with the objective to amend the relevant provisions of the previous Act. The new terms relating to cybercrimes have been added with the stringent punishments under The Information Technology (Amendment) Act, 2008. The Indian Penal Code, 1860 also contains some relevant provisions in order to punish the cybercriminal.

SUGGESTIONS

- The people are not aware about information technology laws are prevailing in India. They do not to how to take action against the cybercriminals. The lack of knowledge on the part of people one of the causes to be victimized of the cybercrime.
- The knowledge of cyber laws can be spread by cyber cell authorities by organizing seminars and conferences in each district. The people who are living in villages they should also be part of these conferences in order to get knowledge of cyber laws. The authorities should use regional language so that the people can understand easily.
- The cyber cells need to be the establishment in every police station. The adequate training to the police officers regarding the investigation of cybercrimes and for redressing the grievances of cyber victims can be proved helpful for curbing the cybercrime. Online complaint mechanism would reduce the harassment of cyber victims. Toll- free number on the site of district cyber cell should be uploaded in order to save the time of the victims and cyber cell's authorities.
- The recent Facebook data leak scam by Cambridge Analytica is an example of lack of security at cyberspace. There is a need that proper security measures should be maintained on social media which necessary for maintaining the privacy of individuals.

- Women victims of cyber crimes should take action against the cyberstalkers under the relevant provisions of the Information Technology Act, 2000 and under the relevant provisions of the Indian Penal Code, 1860.
- With the banning of porn sites at cyberspace the cybercrime would be reduced to some extent. The government of India should take necessary steps with the help of cyberspace authorities to ban the porn sites. The young generation is more prone to cybercrimes and there is a need to make them aware about the pros and cons of cyber-space. The blue whale game took the lives of several children's. At last Indian government took a step with the help of cyber authorities for banning of this game.
- The Information Technology (Amendment) Act, 2008 covers several provisions for mitigating the cyber crimes. It prescribes stringent punishments with heavy fines. The laws alone are not sufficient, the people needed to be more conscious about their privacy and security.

REFERENCES

1. *Verma, Amita, Cyber Crimes and Law, 2009, Central Law Publications, Allahabad, p. 04.*
2. *Malik, Krishna Pal, Computer and Information Technology Law, 2010, Allahabad Law Agency, Faridabad, pp. 08, 09.*
3. *Malik, Krishna Pal, Computer and Information Technology Law, 2010, Allahabad Law Agency, Faridabad, p. 08.*
4. *https://www.legalindia.com/cyber-crimes-and-the-law/: retrieved on April 10, 2018.*
5. *https://www.legalindia.com/cyber-crimes-and-the-law/: retrieved on April 10, 2018.*
6. *http://www.helplinelaw.com/family-law/CCII/cyber-crimes-in-india-what-is-types-web-hijacking-cyber-stalking.html retrieved on April 11, 2018.*
7. *https://www.legalindia.com/cyber-stalking-the-impact-of-its-legislative-provisions-in-india/ retrieved on April 10, 2018.*
8. *https://www.legalindia.com/cyber-stalking-the-impact-of-its-legislative-provisions-in-india/ retrieved on April 10, 2018.*
9. *Section 354 D (Criminal Law (Amendment) Act, 2013) of The Indian Penal Code, 1860 (1) Any man who follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or monitors the use by a woman of the internet, email or any other form of electronic communication, commits the offence of stalking; Provided that such conduct shall not amount to stalking if the man who pursued it proves that— it was pursued for the purpose of preventing or detecting crime and the man accused of stalking had been entrusted with the responsibility of prevention and detection of crime by the State; or it was pursued under any law or to comply with any condition or requirement imposed by any person under any law; or in the particular circumstances such conduct was reasonable and justified. (2) Whoever commits the offence of stalking shall be punished on first conviction with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine; and be punished on a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and shall also be*

liable to fine.

10. *https://www.hindustantimes.com/india-news/president-s-daughter-sharmistha-mukherjee-names-and-shames-pervert-on-facebook/story-8l3io0JaLAaQYuBVDIVt4N.html retrieved on April 25, 2018.*
11. *Section 500 of The Indian Penal Code, 1860.*
12. *Section 509 of The Indian Penal Code, 1860.*
13. *Section 67 of The Information Technology (Amendment) Act, 2008.*
14. *Section 67A of the Information Technology (Amendment) Act, 2008.*
15. *Joshi, Aishwarya,"Identity Theft- A Critical And Comparative Analysis Of Various Laws In India" Journ al On Contemporary Issues of Law (JCIL), Vol. 2 Issue 6, p.01. http://jcil.ls yndicate.com/wpcontent/up loads/2016/ 08/Aishwariya-Joshi.pdf retrieved on April 25, 2018.*
16. *Joshi, Aishwarya,"Identity Theft- A Critical And Comparative Analysis of Various Laws In India," Jour nal On Contemporary Issues of Law (JCIL), Vol. 2 Issue 6, p.03. http://jcil.lsyndi cate.com/wpcontent/uplo ads/2016/08/Aishwariya-Joshi.pdf retrieved on April 25, 2018.*
17. *Pandey, Kumar Askand, Cyber Crime, p.05,06. http://epgp.inflibnet.ac. in/epgpdata/uploads /epgp_content /S0016 08/P001741/M022115/ET/1504181797CyberCrime.pdf retrieved on April 10, 2018.*
18. *Section 66C of The Information Technology (Amendment) Act, 2008.*
19. *https://www.legalindia.com/cyber-crimes-and-the-law/ retrieved on April 10, 2018.*
20. *Verma, Amita, Cyber Crimes and Law, 2009, Central Law Publications, Allahabad, pp. 61, 62.*
21. *Malik, Pal Krishna, Computer & Information Technology Law, 2010, Allahabad Law Agency, Faridabad, pp. 184, 185.*
22. *"2 J&K Students picked up by Delhi's Cyber Crime Cell," The Tribune, April 28, 2018, p. 01.*
23. *https://www.thewindowsclub.com/types-cybercrime / retrieved on April 10, 2018*
24. *https://topyaps.com/top-10-cases-of-hacking-that-were-straight-blackout-for-victims retrieved on April 11, 2018.*
25. *Section 66 of The Information Technology (Amendment) Act, 2008.*
26. *Sarmah, Animesh, Roshmi Sarmah and Amlan Jyoti Baruah , "A brief study on Cyber Crime and Cyber Law's of India," International Research Journal of Engineering and Technology (IRJET), June 2017, Volume: 04 Issue: 06, p. 1634. https://www.irjet.net/archives/V4/i6/IRJET-V4I6303.pdf retrieved on April 10, 2018.*
27. *Jahankhani, Hamid and Amir Al-Nemrat et.al "A Cyber crime Classification and Characteristics," November 2014 , Researchgate, p. 156. https://www.researchgate. net/publication/28048887 3_Cy ber_crime_Cla ssification_and_Characteristicshttp:// retrieved on April 12, 2018.*

28. *Pandey, Kumar Askand, Cyber Crime, p. 27 http://epgp.inflibnet.ac.in/ epgpdata/uploads/epgp_conte nt/S00 1608/P001741/M022115/ET/1504181797CyberCrime.pdf retrieved on April 10, 2018.*
29. *Pandey, Kumar Askand, Cyber Crime http://epgp.inflibnet.ac.in/epgpdata/uploads/epg p_content/S001608 /P001741/M022115/ET/1504181797CyberCrime.pdf retrieved on April 10, 2018.*
30. *Chauhan, M. When Virtual World Meets The Real World: Cyber Crime Induced Drug Trafficking.*
31. *Section 379 of Indian Penal Code, 1860.*
32. *Section 406 of Indian Penal Code, 1860.*
33. *Section 43-A of The Information Technology (Amendment) Act, 2008.*
34. *Section 66 of The Information Technology (Amendment) Act, 2008.*
35. *https://www.legalindia.com/cyber-crimes-and-the-law/: retrieved on April 10, 2018.*
36. *Section 415 of Indian Penal Code, 1860. states that Whoever, by deceiving any person, fraudulently or dishonestly induces the person so deceived to deliver any property to any person, or to consent that any person shall retain any property, or intentionally induces the person so deceived to do or omit to do anything which he would not do or omit if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to that person in body, mind, reputation or property, is said to cheat.*
37. *Section 417 of The Indian Penal Code, 1860.*
38. *https://www.legalindia.com/cyber-crimes-and-the-law/: retrieved on April 10, 2018.*
39. *http://shodhganga.inflibnet.ac.in/bitstream/10603/130487/8/08_chapter%202.pdf pp. 34, 35. Chapter ii Cyber Crime and Its Classification retrieved on April 12, 2018.*
40. *http://shodhganga.inflibnet.ac.in/bitstream/10603/130487/8/08_chapter%202.pdf p. 42, 46 Chapter ii Cyber Crime and Its Classification retrieved on April 12, 2018.*
41. *https://www.legalindia.com/cyber-crimes-and-the-law/: retrieved on April 10, 2018.*
42. *https://www.legalindia.com/cyber-crimes-and-the-law/: retrieved on April 10, 2018.*
43. *https://www.legalindia.com/cyber-crimes-and-the-law/: retrieved on April 10, 2018.*
44. *https://www.legalindia.com/cyber-crimes-and-the-law/: retrieved on April 10, 2018.*
45. *https://www.legalindia.com/cyber-crimes-and-the-law/: retrieved on April 10, 2018.*
46. *https://www.legalindia.com/cyber-crimes-and-the-law/: retrieved on April 10, 2018.*
47. *https://www.legalindia.com/cyber-crimes-and-the-law/: retrieved on April 10, 2018.*

48. *Section 441 of the Indian Penal Code, 1860 provides that whoever enters into or upon property in the possession of another with intent to commit an offence or to intimidate, insult or annoy any person in possession of such property, or, having lawfully entered into or upon such property, unlawfully remains there with intent thereby to intimidate, insult or annoy any such person, or with intent to commit an offence, is said to commit criminal trespass.*

49. *Section 447 of The Indian Penal Code, 1860.*

50. *Section 66 A of The Information Technology (Amendment) Act, 2008. Section 66 A Punishment for sending offensive messages through communication service, etc. Any person who sends, by means of a computer resource or a communication device,- (a) any information that is grossly offensive or has menacing character; or (b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes by making use of such computer resource or a communication device, (c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages (Inserted vide ITAA 2008) shall be punishable with imprisonment for a term which may extend to three years and with fine.*

51. *https://www.legalindia.com/cyber-crimes-and-the-law/: retrieved on April 10, 2018.*

52. *https://www.legalindia.com/cyber-crimes-and-the-law/: retrieved on April 10, 2018.*

53. *http://shodhganga.inflibnet.ac.in/bitstream/10603/130487/8/08_chapter%202.pdf Chapter ii Cyber Crime and Its Classification p. 74 retrieved on April 12, 2018.*

54. *http://shodhganga.inflibnet.ac.in/bitstream/10603/130487/8/08_chapter%202.pdf Chapter ii Cyber Crime and Its Classification p.75 retrieved on April 12, 2018.*

55. *Section 66F of The Information Technology (Amendment) Act, 2008 Punishment for cyber terrorism (1) Whosoever,— (A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by— (i) denying or cause the denial of access to any person authorised to access computer resource; or (ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or (iii) introducing or causing to introduce any computer contaminant, and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disputes or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70; or (B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the state or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or*

otherwise, commits the offence of cyber terrorism.(2) whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

56. *https://www.legalindia.com/cyber-crimes-and-the-law/: retrieved on April 10, 2018.*
57. *https://www.legalindia.com/cyber-crimes-and-the-law/: retrieved on April 10, 2018.*
58. *https://www.legalindia.com/cyber-crimes-and-the-law/: retrieved on April 10, 2018.*
59. *Section 67 B of The Information Technology (Amendment) Act, 2008 prescribes punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form: Whoever,- (a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or (b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or (c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or (d) facilitates abusing children online or (e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees: Provided that the provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form- (i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or (ii) Which is kept or used for bonafide heritage or religious purposes Explanation: For the purposes of this section, 'children' means a person who has not completed the age of 18 years.*
60. *https://www.legalindia.com/cyber-crimes-and-the-law/: retrieved on April 10, 2018.*
61. *https://www.legalindia.com/cyber-crimes-and-the-law/: retrieved on April 10, 2018.*
62. *https://www.legalindia.com/cyber-crimes-and-the-law/: retrieved on April 10, 2018.*
63. *Section 45 of the Information Technology (Amendment) Act, 2008.*