



How ‘IPC’ Goes Hand in Hand with ‘IT Act’ in Dealing with Cyber Crimes.

Gayathri. V

B. Com.LLB(Hons), The Tamil Nadu Dr. Ambedkar Law University, School of Excellence in Law, Chennai.

DOI: <https://doi.org/10.55248/gengpi.2023.4.4.35337>

ABSTRACT:

Crime has its effect on every aspect of field in the society. Among which Cyber Crime has become an emerging one in this digital Era, as many crimes has been happening in cyberspace nowadays, there’s a need for us to know about the cybercrimes and the provisions available under the Information Technology (IT) Act which is specifically enacted to know about the cyber crimes, digital signature, adjudicating authority, etc. And also how Indian Penal Code (IPC), 1860 gives its hands to cover the cyber crimes. And also we will going to see how the Information Technology (amendment) Act has its impact in IPC and the changes or insertion made to IT act, 2000.

Key Words:Cyber Crimes, cyberspace, IT Act,2000, IPC, 1860, IT (amendment) Act, 2008.

INTRODUCTION:

In this modern digitalized world we are more dependent on internet and gadgets like computers, mobile phones and other electronic communications, therefore there is an emerging trend in cyber crimes. So, there is a need for us to understand about the cyber crimes that’s happening around the internet regime in order to be safe while using the same. Most of us might know about cybercrime in general but we would not be aware of the kinds of crimes in the cyberspace, punishments and relevant provisions for the same. Here in this article we will be going to see about the various crimes happening via internet and how the predators be punished. Mainly we are going to get a view on how INDIAN PENAL CODE covers the Cyber Crimes and how Information Technology Act, 2000 and Indian Penal Code, 1860 goes together for providing punishments for various internet crimes.

Cyber Crime – Meaning:

In general crimes are considered to be a violation of the social norms of the society which will be punished based on the laws in existence. We probably would know the crimes that are happening in person e.g. Murder, Theft, Dacoity etc., wherein the predators would go in person by himself for committing the act. Whereas Cyber Crimes are the crimes which happening in the other side of the world i.e., cyberspace. Where the predators will commit the crime through internet mediums and not in person. Wherever the crime happens be it in person or through internet, crime is a crime.

Cyber Crimes are nowhere defined in any statute. We can assume from the term ‘cyber’ that something relating to the internet, computer and many more in the virtual world engaged in internet. It’s just a combination of computer and crime.

» Dr. Debarati Halder and Dr. K. Jaishankar defines Cyber-Crimes as, “offences that are committed against individuals or group of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (chat rooms, emails, notice boards, and groups) and mobile phones (SMS/MMS).”¹

» In the words of Pawan Duggal, “Cybercrime refers to all activities done with criminal intent in cyberspace or using the medium of interest. These could be either the criminal activities in conventional sense or activities newly evolved with the growth of new medium. Any activity, which basically offends the human sensibilities can be included in the ambit of the cybercrimes.”

» Dr. R.K. Tiwari defines, “Cybercrime may be said those species, of which, genus in the conventional crime, and where either the computer is an object or subject of conduct constituting the crime.”²

¹ Jonathan clough, Principles of Cybercrimes 12 (Cambridge publication, 2ndedn 1998)

² Peter Gottschalk, Policing Cyber crime 75 (Lexis Neis publication, 2ndedn 2002)

IPC AND IT ACT:

The Indian Penal Code 1860, is a substantial law which provides provisions explaining various criminal offences and its punishments. And also it covers various aspects of cybercrimes elaborately and also provides provisions for penalizing the same with either imprisonment or fine or both. And some provisions in IPC were amended in order to include digital aspect in the provisions. It's important to note that IPC nowhere uses the word cyber crime even after the amendment made to it by Information Technology (amendment) Act, 2008.

Whereas, **Information Technology Act, 2000** is the very first legislation which deals with technology, computer, internet crimes, digital signature, electronic commerce etc. The IT act got its sources from United Nations Commission on International Trade law (UNCITRAL) Model laws on electronic commerce, and this IT Act was amended in the year 2008, after the Mumbai terrorist attack of November 2008 taken place. This amendment of the Act focused on cyber security and data privacy. Also some cyber crimes like child pornography, cyber stalking and cyber terrorism were added to the act. Thus, IPC and IT Act goes hand in hand by laying provisions for cyber crimes.

CYBER CRIMES:

There are various kinds of cyber crimes in the cyberspace, some of them are as follows:

- » Cyber Stalking
- » Hacking
- » Virus dissemination
- » Cyber terrorism
- » Denial of service
- » Web Jacking
- » Identity theft
- » Data Theft
- » Cheating
- » Cyber Pornography
- » Child Pornography
- » Violation of Privacy
- » Spoofing
- » Defamation
- » Password Sniffing

MEANING AND PROVISIONS:

Now let's see the meaning of the cyber crimes mentioned above and how the Act made cybercrimes a punishable one, and also we will know the relevant provisions in IPC which punishes the cyber crimes and also the provisions given under IT act for various crimes.

CYBER STALKING:

MEANING: **Cyber Stalking** is one of the offences in cyberspace. It's basically a harassment or threat given to an individual via e-mail, internet, computer. It's a behavior of threatening or harassing the other person continuously or persistently over time. Here the email means a message received on a computer or any other communication device which includes attachments in text, image, audio, video and any other e-record which can be transmitted with a message (Explanation under 66A).

PROVISIONS: At the time of enactment of IT act, 2000 there was no provision regarding stalking. Eventually, after the amendment in the year 2008, provision for stalking has been inserted in the act under section **66A** titled as 'Punishment for sending offensive messages through communication service', but this section was struck down in the year 2015 as it violates the constitutional provision. The most used provision for stalking is section **72** – penalty for breach of confidentiality and privacy, section **72A** provides for punishment of disclosure of information in breach of lawful contract.

Whereas, IPC was amended by Criminal Law (amendment) Act 2013, which substituted the title of section **354D** as 'Stalking'. This section also includes stalking via internet, email or other forms of e-communication medium.

PUNISHMENTS: •□ Under section 66A of IT act, the offender shall be punishable with imprisonment for a term which may extend to 3 years and also with fine. (struck down in 2015).

•□ Under section 72 of IT act, the offender shall be punishable with imprisonment for a period which may extend to 2 years or with fine which may extend to 1 lakh rupees or with both.

•□ As per section 72A the person shall be punished with imprisonment extend upto a period of 3 years or with fine which may extend to 1 lakh rupees or with both.

•□ Under IPC sec 354D the punishment for the offender in case of first conviction (cognizable and bailable) is- imprisonment of period extend upto 3 years and shall also be liable to fine.

In case of habitual offender i.e., second or subsequent conviction the imprisonment shall be for a period extend upto 5 years and shall also be liable to fine.

HACKING:

MEANING: Hacking is also a form of cyber offence. Hacking is an act where the predator will get into the computer or other form of networks without permission. It's something in which he gains access in unlawful manner.

PROVISION: •□ Sections 43 and 66 provides compensation and penalty for the crimes which cause damage to computer, computer system , etc.

•□ Under section 43 of the Act it lists various crimes which cause damage to computer. And in section 66 it provides punishment for those crimes which falls under section 43.

•□ prior to the amendment of 2008, section 66 titled as 'Hacking with computer system', which provides meaning of hacking under clause (1) and punishment under clause (2). After amendment 2008 (w.e.f. 2009) section 66 was amended and forthwith it was titled as 'computer related offences' and the content under the section gives only punishment for those crimes comes under the ambit of sec 43. There after Hacking comes under the sphere of sec 43.

PUNISHMENT: Punishment is given under section 66 of IT act. The section states that, "If any person, dishonestly or fraudulently, does any act which falls under section 43, then he shall be punishable with imprisonment for a term which may extend to 3 years or with fine which may extend to 5 lakh rupees or with both."

Under the explanation of this section, the act states that the words 'dishonestly', 'fraudulently' for the purpose of this section shall have the meaning which is given under Indian Penal Code, 1860. (Section 24 gives the meaning of the word 'dishonestly' and section 25 assigns the meaning of the word 'fraudulently'.

VIRUS DISSEMINATION:

MEANING: Dissemination is again a tool to the offenders to commit cyber crime. In which the offender will pass-on/inject virus in other person's computer without the knowledge of the user. Computer viruses are the written program which have the capacity to alter or destroy the files and data in the user's computer. It can be in the form of time bomb, virus, worm, Trojan etc.

PROVISION: section 43 and section 66 provides for compensation and punishment for various crimes which causes damage to computer, computer system. Virus Dissemination will fall under the section 43. Section 43 (c) states that, without permission of the owner, if any person introduces or causes to be introduced any virus into computer is a crime which cause damage to computer.

PUNISHMENT: Section 66 provides for punishment for Virus Dissemination which falls under section 43. The punishment is, the offender shall be punishable with imprisonment for a period which may extend to 3 years or fine which may extend to 5 lakh rupees or with both.

CYBER TERRORISM:

MEANING: Cyber terrorism is also a type of cyber crime. It's considered to be one of the rapidly increasing crime in cyberspace. In this type of cyber offence the predator will cause fear or cause intimidation which result in generating fear to the victim.

Cyber terrorism was defined by a defense analyst named, Dorothy Denning. In his words, cyber terrorism means – "Unlawful attacks and threats of attacks against computers, networks and information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives."

PROVISION: •□ Information Technology (Amendment) Act, 2008, under section 66F it gives punishment for cyber terrorism. The meaning of cyber terrorism under this section is that, "whoever, with an intent to threaten the unity, integrity, security or sovereignty of India or any section of people by – (i) denying or cause denial of access to any person authorized to access computer resource, or

(ii) attempting to penetrate or access computer resource without authorization or exceeding authorized access, or

(iii) introducing or causing to introduce any computer contaminant.”³

PUNISHMENT: Clause (2) of section 66F provides the punishment for cyber terrorism, according to the clause, any person who commits cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

DENIAL OF SERVICE ATTACKS:

MEANING: Denial of service attacks also falls under the classification of cyber crimes. It's commonly known as 'DOS', it helps to make the server inaccessible to the user. There are two ways in which DOS attacks happens, one is by flooding services and another one is crashing the services. Flooding the services generally occurs when the service receives so much messages which ultimately result in slowing down the server and even the server will stop because of flooding of messages. Types of DOS attacks includes SYN overflow, Smurf attack and the most common form of DOS attacks is the buffer overflow attacks.

PROVISION: Section 66 provides for punishment for computer related offences which falls under the sphere of section 43. Section 43(f) includes the denial of access to the person who is authorized to access any computer. Section 66F also applies to denial of service attacks.

Section 66 provides punishment of cyber terrorism. Under sec 66F(1) (A) (i) states that, if any person denies access to any other person who has authorized access over the computer resource is said to be an offence.

PUNISHMENT: Punishment under section 66 – imprisonment for a period which may extend to 3 years or fine which may extend to 5 lakh rupees or both.

Punishment given section 66F for cyber terrorism will also applies to the crime of denial of access attacks. It gives punishment which may extend to imprisonment for life.

WEB JACKING:

MEANING: Web Jacking is a tool used by the offender in order to attack the user and extract or steal sensitive data from him. It's a kind of trap wherein the attacker will get access/control of other person's website. It's similar to hi-jacking, in fact we can say that web jacking is derived from hi-jacking.

PROVISION: There is no express provision for web jacking. However, section 383 of IPC, 1860 which deals with extortion, applies to web jacking. This section states that, 'Whoever intentionally puts any person in fear of any injury to that person, or to any other, and thereby dishonestly induces the person so out in fear to deliver to any person any property or valuable security, or anything signed or sealed which may converted into valuable security, commits "extortion".'⁴

PUNISHMENT: Punishment under 384 of IPC, it gives punishment for extortion. The punishment under this section includes imprisonment for a term which may extend to 3 years or fine or both.

IDENTITY THEFT:

MEANING: Identity theft is a common form of cyber crime, in which the offender will steals and fraudulently use the victim's personal information for committing a crime. The personal information can be the victim's password, electronic signature, credit card information, bank account details etc.

PROVISION: Section 66C of Information Technology Act 2000 provides for punishment of identity theft. If any person use electronic signature, password or any other unique identification feature of any other person fraudulently or dishonestly, then it's a punishable offence.

Section 464(c) of IPC states that if any person fraudulently or dishonestly affixes any electronic signature on any electronic record and 464 (d) if any person fraudulently or dishonestly makes any mark which denotes the authenticity of the electronic signature,

With and intention to causing it to be believed that such a electronic signature was made by the authority of a person⁵. Under explanation 2 of the same section it stated it amounts to Forgery.

PUNISHMENT: Under section 66C punishment is, imprisonment for a period which may extend to 3 years and shall also be liable to fine which may extend to 1 lakh rupees.

Under 465 it provides for punishment of Forgery. The punishment is for a period which may extend to 2 years or with fine or both.

³ Section 66F, Information Technology Act, 2000.

⁴ Section 383, Indian Penal Code, 1860.

⁵ Section 464, Indian Penal Code, 1860.

DATA THEFT:

MEANING: **Data Theft** is again a cyber crime wherein the offenders will get access to your (user's) private information which you (user) don't want to share publicly. It's generally a breach of confidentiality or privacy which is punishable under the Act. It includes passwords, algorithms technologies. Mainly the offender steals information by bigger organizations to harm them in an unethical manner.

PROVISION: ■□ Section 43(b) of the IT act, it states that, when a person without the permission of the owner, downloads extract or copy any data, computer data base or information from computer which also includes information from any computer system or network, any data stored in a removable medium.

■□ Section 65 titled 'tampering of computer source document', states that if any person knowingly or intentionally destroy, conceals or alter any computer, computer system or network, or computer code, program then it's an offence.

■□ Section 72 of IT Act states that, if any person without the permission or knowledge of the concerned person access any electronic record, information, register etc., and discloses the same to any other person is a punishable offence.

■□ IPC section 378 discusses about theft. As per this section, if any person dishonestly takes any movable property from the possession of the owner without his consent is said to commit theft. Under sec 22 of the IPC provides for the meaning of movable property, under which it states that movable property includes corporeal property. Therefore this section also includes intangible property. Also, under section 43(b) of IT act includes any data stored in removable medium, which automatically falls under the section 378 which includes movable property.

PUNISHMENT: ■□ As per section 66, provides punishment for any offence falls under sec 43. Therefore punishment as per sec 66 is imprisonment for a term which may extend to 3 years or with fine which may extend to 5 lakh rupees or both.

■□ As per section 65 of IT Act, punishment is imprisonment for a period extend to 3 years or fine which may extend to 2 lakh rupees or both.

■□ Section 72 provides punishment for breach of confidentiality and privacy as, imprisonment which may extend upto 2 years or with fine which may extend upto 2 lakh rupees or both.

■□ According to section 379 of IPC, the punishment for theft is imprisonment upto 3 years or with fine or both.

CYBER PORNOGRAPHY:

MEANING: **Cyber Pornography** also falls under the ambit of cyber crime. Any act of transmitting, distributing or publishing any material which contain sexually explicit act then it is an offence and also shall be punishable under the Act. The transmission of cyber Pornography through mail, or any mode of instant messaging medium is said to be an offence, and also publishing any pornography content in online platform is considered to be an offence. However, viewing cyber Pornography is legal in India. Merely browsing, downloading and viewing a sexual content does not amount to an offence.

In case of **Child Pornography**, even browsing, viewing, downloading, publishing or transmitting the content of child pornography is considered to a punishable offence.

PROVISION: ■□ Section 67 provides 'punishment for publishing or transmitting obscene material in electronic form.'

■□ Section 67A of IT Act provides 'Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.' As meaning of the cyber pornography is explained above, this provision gives punishment for the same.

■□ Section 67B provides 'punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.' Basically this provision punished child pornography. Also in this section the term 'children' means person less than 18 years old.

[Under this section and sec 67, 67A, it doesn't extend to book, pamphlet, drawing, painting, figure which is published for public good]

■□ IPC section 293 Which prohibit and punishes the sale, etc., of obscene objects to young person. Under this section the person should be of age less than 22 years old.

■□ As per section 292 of IPC, it punishes any person for sale, etc., of obscene books etc.

PUNISHMENT: ■□ Section 67 gives punishments for publishing or transmitting obscene material in electronic form. The punishment includes imprisonment of a period which may extend upto 3 years or fine which may extend 5 lakh rupees in case of first conviction. And in case of habitual offender, the punishment is imprisonment which may extend to 5 years or fine which may extend to 10 lakh rupees.

■□ As per section 67A of IT act, the punishment is imprisonment for a period which may extend to 5 years and with fine which may extend upto 10 lakh rupees in case of first conviction. And in case of second or subsequent conviction imprisonment may extend upto 7 years and fine may extend upto 10 lakh rupees.

▪□ Section 67B provides punishment for a period of imprisonment which may extend upto 5 years or fine which may extend to 10 lakh rupees in case of first conviction. And incase of second or subsequent conviction the punishment is imprisonment for a period which may extend upto 7 years and fine which may extend upto 10 lakh rupees.

▪□ As per sec 293 of IPC, punishment for the offender is imprisonment for a term which may extend to 3 years and fine which may extend to 2000 rupees in case of first conviction, and incase of subsequent conviction imprisonment may extend upto 7 years and fine which may extend upto 5000 rupees.

▪□ According to section 292 of IPC, punishment includes imprisonment for a period which may extend to 2 years and fine which may extend upto 2000 rupees incase of first conviction. And in case of habitual offender the punishment is imprisonment for a term which may extend to 5 years and fine which may extend to 5000 rupees.

VIOLATION OF PRIVACY:

MEANING: **Violation of Privacy** is also a punishable crime in cyberspace. The IT act, 2000, states that, if any person captures, publishes or transmits the image of a private area of any other person whether knowingly or intentionally, then it's a crime which shall be punished with imprisonment.

PROVISION: ▪□ Section 66E of IT Act, 2000 provides 'punishment for violation of privacy.' This section states that, if any person intentionally or knowingly captures, publishes or transmits the image of private area of any other person is a punishable crime. Also under explanation of this section, the act provides for meaning of the terms – transmits, capture, private area, publishes and under the circumstances violation privacy.

▪□ IPC section 292 states, if any person sells, hires or publicly exhibit or has in possession any obscene book, pamphlet, paper, drawing, painting or any other object is said to be an punishable offence. This section does not include any above mentioned act for bona-fide religious purpose, monuments, temples for any religious purpose and objects for general concern.

PUNISHMENT: ▪□ According to section 66E of IT Act, punishment is imprisonment which may extend to period of 3 years or with fine not exceeding 2 lakh rupees or with both.

▪□ As per section 292 of IPC, the punishment is imprisonment of period which may extend to 2 years and with fine which extend to 2000 rupees in case of first conviction. And in case of subsequent conviction punishment is imprisonment for a term which may extend to 5 yerss and with fine which may extend to 5000 rupees.

CYBER DEFAMATION:

MEANING: **Cyber Defamation** is a crime in the cyberspace. If a false accusation made on someone for something which cause damage to their reputation, or if it is likely to diminish their dignity or destroying their self respect or likely to harm their character in public sphere, it is said to be defamation. If such a defamation happens on online platforms then it is said to be a cyber defamation.

PROVISION: ▪□ Section 66A of IT Act, provides for 'punishment for sending offensive messages through communication service etc.,' In the words of this section, if any person sends any information persistently which is offensive or has menacing character or the sender knows such information which he send is false, just for a purpose of causing hatred, harm or ill will by using any electronic medium e.g.: computer, or other communication device is said to be punishable offence.

▪□ Under IPC section 499 discuss about defamation. If any person by words, signs, or visible representation, makes or publishes anything in the regard of any other person intending to harm the reputation of that concerned person is a punishable offence.

▪□ Section 469 of IPC, it provides punishment for 'Forgery for purpose of harming reputation.' As per this section, if any person knowingly attempt forgery, intending that the electronic record or document shall harm the reputation of any other person, is said to be an punishable offence.

PUNISHMENT: ▪□ As per section 66A of IT act, punishment is imprisonment for a period upto 3 years and with fine.

▪□ Acc to section 500 of IPC the person cause defamation shall be punishable with imprisonment which may extend to a period of 2 years or with fine or both.

▪□ Section 469, the punishment is imprisonment for a period which may extend to 3 years and shall also be liable to fine.

SPOOFING:

MEANING: **Spoofing** is also a cyber offence, wherein the intruder tries to be/ falsely exhibit himself as someone else by introducing fake traffic. Spoofing is a identity theft or sometimes it can be partly called as phishing. It will come under the sphere of identity theft is the offender uses the identity of a legitimate user, and it will fall under the ambit of phishing when the offender tries to steal the personal information like bank account details of the user. And both the Acts i.e., IPC and IT Act provides punishment for e-mail spoofing.

PROVISION: ■ Under section 66C of IT act, it provides ‘punishment for identity theft.’ Under this section it provides punishment for e-mail spoofing. If any person uses any identification feature of any other person then it’s a punishable offence.

- Under section 66A the offender shall be punishable for spreading false information.

- Under section 66D it provides ‘punishment for cheating by personation by using computer resources.’ Whoever cheats another person by personation then it’s a punishable offence.

- As per IPC section 465, it provides punishment for Forgery.

- Section 468 provides for ‘Forgery for purpose of cheating.’ It states that if any person uses forged electronic record for the purpose Cheating, then it’s a punishable offence.

PUNISHMENT: ■ As per section 66C of IT act, punishment is imprisonment for a period which may extend upto 3 years and shall also be liable to fine which may extend to 1 lakh rupees.

- Acc to section 66A of IT act, the offender is punishable with imprisonment for a period which may extend to 3 years and with fine.

- Under section 66D the offender is punishable for personation with imprisonment for a period upto 3 years and shall be liable to fine which may extend to 1 lakh rupees.

- Under section 465 of IPC, for Forgery a person shall be punished with imprisonment for a period upto 2 years or with fine.

- Section 468 of IPC states the punishment for the offender as imprisonment for a term which may extend to 7 years and shall be liable to fine.

OTHER OFFENCES AND PROVISIONS:

1. If a person receives any stolen computer or computer resources or any other communication devices in dishonest manner knowing that it’s a stolen property, then it’s a punishable offence.

PROVISION: ■ Section 66B of IT act, provided for punishment for receiving stolen property. The punishment is imprisonment for a period which may extend to 3 years or with fine which may extend to 1 lakh rupees or both.

- Section 411 of IPC, provides for the provision of ‘Dishonestly receiving stolen property.’ If any person receives any stolen property knowing that it was a stolen property then it shall be punishable for imprisonment for a term which may extend to 3 years or with fine or both.

2. Sending offensive messages through any communication devices is an punishable offensive under IPC, 1860.

PROVISION: ■ Section 500 of IPC provides for punishment for defamation. Under this section the punishment is imprisonment for a term which may extend to 2 years or fine or both.

- As per sec 504, IPC provides a provision titled ‘Intentional insult to provoke breach of the peace.’ If any person insult any other person which in a result cause him breach of peace is a punishable offence. The punishment if imprisonment for a period upto 2 years or fine or both.

- Section 507 of IPC provides for punishment for ‘criminal intimidation by an anonymous communication.’ As per this provision if a person commits any intimidation, also hides his name or conceal the place where resides and gives the threat is said to a punishable offence. The punishment is for a term upto 2 years and along with the punishment provided under section 506.

- Section 508 of IPC states that, ‘word, gesture or act intended to insult the modesty of a woman.’ If any person gives any sign or utter any word or sound with an intention to insult the modesty of the modesty then the punishment is for a period upto 3 years and also liable to fine.

3. If any person misuse wi-fi connection and used it against State, then it’s a punishable offence 66 of IT act. The punishment is for a period extend to 3 years or with fine which may extend to 5 lakh rupees or both. Also under section 66F of IT act which provided for ‘punishment for cyber terrorism’ also applies here. According to this provision the punishment is imprisonment which may extend to life imprisonment.

4. Incase of copyright © infringement, there are provisions under IT act and Copyrights Act.

PROVISION: ■ As per sec 66 of IT act the punishment if for a period which may extend to 3 years or fine which may extend to 5 lakh rupees or both

- Acc to section 63, 63B Copyrights Act, 1957 the infringement can be tried. As per sec 63B the punishment is imprisonment not less then 7 days but which may extend upto 3 years and fine not less then 50,000 rupees and which my extend upto 2 lakh rupees. The imprisonment under section 63 is for term not less then 6 months and which may extend to 3 years and with fine not less then 50,000 rupees and which my extend upto 2 lakh rupees. Also this section different punishment in case the infringement doesn’t take place in the course of trade. In such case the imprisonment shall be for a period of less than 6 months or fine less than 50,000 rupees.

5. Incase of theft of a hardware of a computer then it’s a punishable offence under IPC. And the provision attract this crime is section 379 which provides for ‘punishment for theft.’ As per this section punishment is imprisonment for a period extend to 3 years or fine or both.

CONCLUSION:

There are many crimes happening around us in this digital Era. So it is necessary for us to understand the crimes that can be take place in the cyberspace and how it can be made punishable under IT Act and IPC act. Mainly in this article we have seen most of the crimes that can be commonly happen via computer and its resources or though any other communication devices. And also we saw how Indian Penal Code is used to cover various cyber crimes even though the act doesn't has a express domain to deal with cyber crimes, and provisions of IPC applied by courts based on facts and circumstances And even IT act doesn't cover many cyber crimes, and after amendment in 2008, it inserted provisions to cover many crimes which have overriding effect on IPC.

REFERENCES:

1. Information Technology Act, 2000
2. Information Technology (amendment) Act, 2008
3. Indian Penal Code, 1860