CYBER CRIMES UNDER THE IPC AND IT ACT - AN OVERVIEW

Written by ***Dr. Rekha Chavan***

Assistant Professor of Law, Government Law College, Hassan, Karnataka, India

ABSTRACT

Crime is both a social and economic phenomenon. It is as old as human society. Crime in any form adversely affects all the members of the society. In developing economies, cyber-crime has increased at rapid strides, due to the rapid diffusion of the Internet and the digitisation of economic activities. computer offences are called by several names: Cyber-crimes, computer crimes and computer related crimes. They are also known as computer misuse and computer abuse. These offences specified in Information Act if they are read with any of the crimes specified in the Indian Penal Code such as fraud, mischief, theft etc., they became offences punishable through Criminal court with imprisonment and fine.

Keywords: Cyber-crime, Internet, Computer, Hacking, Phishing, Cyber Terrorism.

INRODUCTION

Computers, the internet and electronic communications play an ever-increasing part in all our lives, with the use of the internet in the home, at work or in educational establishments now standard and continuing to grow. The Internet is one of the fastest-growing areas of technical infrastructure development. Today, information and communication technologies (ICTs) are omnipresent and the trend towards digitization is growing. The world has well and truly entered the digital age where technology is ever-present and all pervasive. The development of technological innovations facilitates our everyday lives. But they also make significant contributions to criminality. Cybercrime has become a serious problem globally.

Crime in a developing nation is a hindrance to its development. It not only adversely affects all the members of the society but it also pulls down the economic growth of the country. Computer Technology provided a boost to the human life. It made the life of human being easier and comfortable. It not only added speed to the life of human being, but it also added accuracy and efficiency. But this computer was exploited by the criminals. This illegal use of computers for commission of crime leads to Cyber Crime. To combat Cyber Crime India got armed herself with The Information Technology Act 2000.

To combat Cyber Crime India got armed herself with The Information Technology Act 2000. This act got drastically amended in year 2008. The Amended Information Technology Act is not only effective than the previous Act it is more powerful and stringent than the previous one.

MEANING OF CYBER CRIMES

The term "cyber-crimes" is not defined in any statute or rulebook. Offence or crime has been dealt with elaborately listing various acts and the punishments for each, under the Indian Penal Code, 1860 and quite a few other legislations too. Hence, to define cyber crime, we can say, it is just a combination of crime and computer. The word "cyber" is slang for anything relating to computers, information technology, internet and virtual reality. Therefore, it stands to reason that "cyber-crimes" are offences relating to computers, information technology, internet and virtual reality. One finds laws that penalise cyber-crimes in a number of statutes and even in

regulations framed by various regulators. The Information Technology Act, 2000 ("IT Act") and the Indian Penal Code, 1860 ("IPC") penalise a number of cyber-crimes.

In the words of **Dr. Debarati Halder** and **Dr. K. Jaishankar**, cybercrimes are "Offences that are committed against individuals or groups 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)."[i]

In the words of **Pawan Duggal,** "Cyber crime refers to all the activities done with criminal intent in cyberspace or using the medium of internet. These could be either the criminal activities in the conventional sense or activities, newly evolved with the growth of the new medium. Any activity, which basically offends human sensibilities, can be included in the ambit of cybercrimes." In the words of **Dr. R.K. Tewari**, "cyber crime may be said those species, of which, genus in the conventional crime, and where either the computer is an object or subject of the conduct constituting crime".[ii]

COMMON FORMS OF CYBERCRIME

- Phishing: using fake email messages to get personal information from internet users;
- Misusing personal information (identity theft);
- Hacking: shutting down or misusing websites or computer networks;
- Spreading hate and inciting terrorism;
- Distributing child pornography;

Hacking:

Amongst all types of cyber crime it is the most dangerous and serious threat to the internet and e-commerce. Hacking refers to the secretively breaking into the computer system and stealing valuable data from the system without any permission. Spreading computer virus: It refers a set of Cyber instructions which are able to perform some malicious operations. Viruses stop the normal functioning of the system programs and insert few abnormalities. A computer virus can be spread through- Emails, CDs, pen drives (secondary storage), Multimedia, Internet[iii]

Phishing:

Phishing refers to stealing information's like passwords, credit card details, usernames etc of target person/persons over the internet. Phishing is carried out by email spoofing and instant messaging. In this type direct link which directs the targeted persons to the fake page which looks and feels identical to the actual one.[iv]

Cyber Defamation:

functioning of the system programs and insert few abnormalities. A computer virus can be spread through- Emails, CDs, pen drives (secondary storage), Multimedia, Internet.[v]

Cyber Staking:

Cyber stalking is use of the Internet or other electronic means to stalk someone. This term is used interchangeably with online harassment and online abuse. Stalking generally involves harassing or threatening behavior that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property.[vi]

Cyber Trafficking:

It may be trafficking in weapons, drugs, human beings, which affect the large numbers of persons.[vii]

Web Jacking:

The term Web jacking has been derived from hi jacking. In this offence the attacker creates a fake website and when the victim opens the link a new page appears with the message and they need to click another link. If the victim clicks the link that looks real, he will be redirected to a fake page. These types of attacks are done to get entrance or to get access and controls the site of another. The attacker may also change the information of the victim's webpage [viii]

CYBER CRIMES WITH IPC IMPLICATIONS

Apart from punishments in IT Act, 2000, there are certain crimes that are attracted by IPC provisions as well. The following is the enumeration of the IPC provisions along with various cyber crimes that are attracted by respective Sections and the punishment for the same.

- **Section 292 of IPC:** Although this Section was drafted to deal with the sale of obscene material, it has evolved in the current digital era to be concerned with various cybercrimes. The publication and transmission of obscene material or sexually explicit act or exploit acts containing children, etc which are in electronic form are also governed by this section. Though the crimes mentioned above seem to be alike, they are recognized as different crimes by the IT Act and IPC. The punishment imposed upon the commission of such acts is imprisonment and fine up to 2 years and Rs. 2000. If any of the aforementioned crimes are committed for the second time, the imprisonment could be up to 5 years and the fine could be imposed up to Rs. 5000.
- **Section 354C of IPC:** The cybercrime dealt with under this provision is capturing or publication of a picture of private parts or acts of a woman without such person's consent. This section exclusively deals with the crime of 'voyeurism' which also recognizes watching such acts of a woman as a crime. If the essentials of this Section (such as gender) are not satisfied, Section 292 of IPC and Section 66E of IT Act, 2000 is broad enough to take the offenses of a similar kind into consideration. The punishment includes 1 to 3 years of imprisonment for first-time offenders and 3 to 7 years for second-time offenders.
- **Section 354D of IPC**: This section describes and punishes 'stalking' including both physical and cyberstalking. If the woman is being monitored through electronic communication, internet, or email or is being bothered by a person to interact or contact despite her disinterest, it amounts to cyber-stalking. The latter part of the Section states the punishment for this offense as imprisonment extending up to 3 years for the first time and 5 years for the second time along with a fine imposed in both the instances. In the case of *Kalandi Charan Lenka v. The State of Odisha*,[ix] the victim received certain obscene messages from an unknown number which are damaging her character. Moreover, emails were sent and the fake Facebook account

was created by the accused which contained morphed pictures of the victim. Hence, the accused was found prima facie guilty for cyberstalking by the High Court under various provisions of IT Act and Section 354D of IPC

- **Section 379 of IPC**: If a mobile phone, the data from that mobile or the computer hardware is stolen, Section 379 comes into the picture and the punishment for such crime can go up to 3 years of imprisonment or fine or both. But the attention must be given to the fact that these provisions cannot be applied in case the special law i.e IT Act, 2000 provisions are attracted. In this regard, in the case of *Gagan Harsh Sharma v. The State of Maharashtra*,[x] one of the employers found that the software and data were stolen and someone has breached the computers and gave access to sensitive information to the employees. The employer gave information to the police and they filed a case under Section 379, 408, and Section 420 of IPC and various other IT Act provisions. The question in front of the court is whether the police can file a case under IPC or not. The court decided that the case cannot be filed based on the IPC provisions as the IT Act has an overriding effect.
- **Section 411 of IPC:** This deals with a crime that follows the offenses committed and punished under Section 379. If anyone receives a stolen mobile phone, computer, or data from the same, they will be punished in accordance with Section 411 of IPC. It is not necessary that the thief must possess the material. Even if it is held by a third party knowing it to be others, this provision will be attracted. The punishment can be imposed in the form of imprisonment which can be extended up to 3 years or fine or both.
- **Section 419** and **Section 420 of IPC**: These are related provisions as they deal with frauds. The crimes of password theft for the purpose of meeting fraudulent objectives or the creation of bogus websites and commission of cyber frauds are certain crimes that are extensively dealt with by these two sections of IPC. On the other hand, email phishing by assuming someone's identity demanding password is exclusively concerned with Section 419 of IPC. The punishments under these provisions are different based upon the gravity of the committed cybercrime. Section 419 carries a punishment up to 3 years of imprisonment or fine and Section 420 carries up to 7 years of imprisonment or fine.

- **Section 465 of IPC**: In the usual scenario, the punishment for forgery is dealt with in this provision. In cyberspace, the offenses like email spoofing and preparation of false documents are dealt with and punished under this Section which imbibes the imprisonment reaching up to 2 years or fine or both. In the case of *Anil Kumar Srivastava v. Addl Director, MHFW,* [xi]the petitioner electronically forged signature of AD and later filed a case making false allegations about the same person. The Court held that the petitioner was liable under Section 465 as well as under Section 471 of IPC as the petitioner also tried to use it as a genuine document.
- **Section 468 of IPC**: If the offenses of email spoofing or the online forgery are committed for the purpose of committing other serious offenses i.e cheating, Section 468 comes into the picture which contains the punishment of seven years of imprisonment or fine or both.
- **Section 469 of IPC:** If the forgery is committed by anyone solely for the purpose of disreputing a particular person or knowing that such forgery harms the reputation of a person, either in the form of a physical document or through online, electronic forms, he/she can be imposed with the imprisonment up to three years as well as fine.
- **Section 500 of IPC**: This provision penalizes the defamation of any person. With respect to cybercrimes, sending any kind of defamatory content or abusive messages through email will be attracted by Section 500 of IPC. The imprisonment carried with this Section extends up to 2 years along with fine.
- **Section 504 of IPC:** If anyone threatens, insults, or tries to provoke another person with the intention of effecting peace through email or any other electronic form, it amounts to an offense under Section 504 of IPC. The punishment for this offense extends up to 2 years of imprisonment or fine or both.
- **Section 506 of IPC**: If a person tries to criminally intimidate another person either physically or through electronic means with respect to the life of a person, property destruction through fire or chastity of a woman, it will amount to an offense under Section 506 of IPC and punishment of imprisonment where the maximum period is extended up to seven years or fine or both.
- **Section 509 of IPC**: This Section deals with the offense of uttering a word, showing a gesture, and committing an act that has the potential to harm the modesty of a

woman. It also includes the sounds made and the acts committed infringing the privacy of a woman. If this offense is committed either physically or through electronic modes, Section 509 gets attracted and the punishment would be imprisonment of a maximum period of one year or fine or both.

CYBER CRIMES AND IT ACT

Hacking and Data Theft: Sections 43 and 66 of the IT Act penalise a number of activities ranging from hacking into a computer network, data theft, introducing and spreading viruses through computer networks, damaging computers or computer networks or computer programmes, disrupting any computer or computer system or computer network, denying an authorised person access to a computer or computer network, damaging or destroying information residing in a computer etc. The maximum punishment for the above offences is imprisonment of up to 3 (three) years or a fine or Rs. 5,00,000 (Rupees five lakh) or both.

Receipt of stolen property: Section 66B of the IT Act prescribes punishment for dishonestly receiving any stolen computer resource or communication device. This section requires that the person receiving the stolen property ought to have done so dishonestly or should have reason to believe that it was stolen property. The punishment for this offence under Section 66B of the IT Act is imprisonment of up to 3 (three) years or a fine of up to Rs. 1,00,000 (Rupees one lakh) or both.

Identity theft and cheating by personation: Section 66C of the IT Act prescribes punishment for identity theft and provides that anyone who fraudulently or dishonestly makes 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 3 (three) years and shall also be liable to fine which may extend to Rs. 1,00,000 (Rupees one lac).

Section 66D of the IT Act prescribes punishment for 'cheating by personation by using computer resource' and provides that any person who 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 3 (three) years and shall also be liable to fine which may extend to Rs. 1,00,000 (Rupees one lakh).

Obscenity: Sections 67, 67A and 67B of the IT Act prescribe punishment for publishing or transmitting, in electronic form: (i) obscene material; (ii) material containing sexually explicit act, etc.; and (iii) material depicting children in sexually explicit act, etc. respectively. The punishment prescribed for an offence under section 67 of the IT Act is, on the first conviction, imprisonment of either description for a term which may extend to 3 (three) years, to be accompanied by a fine which may extend to Rs. 5,00,000 (Rupees five lakh), and in the event of a second or subsequent conviction, imprisonment of either description for a term which may extend to 5 (five) years, to be accompanied by a fine which may extend to Rs. 10,00,000 (Rupees ten lac). The punishment prescribed for offences under sections 67A and 67B of the IT Act is on first conviction, imprisonment of either description for a term which may extend to 5 (five) years, to be accompanied by a fine which may extend to Rs. 10,00,000 (Rupees ten lac) and in the event of second or subsequent conviction, imprisonment of either description for a term which may extend to 7 (seven) years and also with fine which may extend to Rs. 10,00,000 (Rupees ten lakh).

Section 43(h) of the IT Act: Section 43(h) read with section 66 of the IT Act penalises an individual who charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network. A person who tampers with the computer system of an electricity supplier and causes his neighbour to pay for his electricity consumption would fall under the aforesaid section 43(h) of the IT Act.

Section 65 of the IT Act: Section 65 of the IT Act prescribes punishment for tampering with computer source documents and provides that any person who knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code (i.e. a listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form) 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 for up to 3 (three) years or with a fine which may extend to Rs. 3,00,000 (Rupees lac) or with both.

Violation of privacy: Section 66E of the IT Act prescribes punishment for violation of privacy and provides that any person who 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 3 (three) years or with fine not exceeding Rs. 2,00,000 (Rupees two lakh) or with both.

Section 67C of the IT Act: Section 67C of the IT Act requires an 'intermediary' to preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe. The section further provides that any intermediary who intentionally or knowingly contravenes this requirement shall be punished with imprisonment for a term which may extend to 3 (three) years and also be liable to a fine. An 'intermediary' with respect to any particular electronic record, has been defined in the IT Act to mean any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes.

Cyber terrorism: Section 66F of the IT Act prescribes punishment for cyber terrorism. Whoever, 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, denies or causes the denial of access to any person authorized to access a computer resource, or attempts to penetrate or access a computer resource without authorisation or exceeding authorised access, or introduces or causes the introduction of 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 disrupts 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 critical information infrastructure, is guilty of 'cyber terrorism'. Whoever 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 for 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, is also guilty of 'cyber terrorism'.

Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

WHETHER COMPOUNDABLE, COGNIZABLE AND BAILABLE

Section 77A of the IT Act provides that, subject to certain exceptions, all offences under the IT Act for which the punishment is imprisonment for a term of 3 (three) years or less, are compoundable. The provisions of sections 265B and 265C of the Code of Criminal Procedure, 1973 ("CrPC") shall apply with respect to such compounding.

Section 77B of the IT Act provides that notwithstanding anything contained in the CrPC, all offences punishable with imprisonment of 3 (three) years and above under the IT Act shall be cognizable and all offences punishable with imprisonment of 3 (three) years or less shall be bail able.

Most of the cyber-crimes covered under the IT Act are punishable with imprisonment of 3 (three) years or less. The cyber-crimes which are punishable with imprisonment of more than 3 (three) years are:

a. publishing or transmitting obscene material in electronic form under section 67 of the IT Act;
b. publishing or transmitting of material containing sexually explicit act, etc., in electronic form under section 67A of the IT Act;
c. publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form under section 67B of the IT Act; and
d. cyber terrorism under section 66F of the IT Act.

All of the cyber-crimes under the IPC are bail able other than offences under section 420 (*cheating and dishonestly inducing delivery of property*), section 468 (*forgery for the purpose of cheating*), section 411 (*dishonestly receiving stolen property*), section 378 (*theft*) and section

409 (*criminal breach of trust by public servant, or by banker, merchant or agent*), which are non-bail able.

Offences under sections 463 and 465 (*forgery*), sections 425 and 426 (*mischief*), section 468 (*forgery for the purpose of cheating*), section 469 (*forgery for the purpose of harming reputation*) and section 292 (*sale, etc., of obscene books, etc.*) of the IPC are non-compoundable offences while offences under sections 378 and 379 (*theft*), 420 (*cheating and dishonestly inducing delivery of property*), sections 425 and 426 (*mischief when the only loss or damage caused is loss or damage to a private person*), section 509 (*word, gesture or act intended to insult the modesty of a woman*), section 411 (*Dishonestly receiving stolen property*) and section 419 (*Punishment for cheating by personation*) of the IPC are compoundable offences. Of these, offences under sections 420 and 509 can be compounded only with the permission of the court. Most of the cyber crimes under the IPC are cognizable other than the offences under sections 425 and 426 (*mischief*) and sections 463 and 465 (*forgery*) which are non-cognizable.

The overlap between the provisions of the IPC and the IT Act may sometimes lead to an anomalous situation wherein certain offences are bail able under the IPC and not under the IT Act and vice versa and certain offences are compoundable under the IPC and not under the IT Act and vice versa. For instance, in case of hacking and data theft, offences under sections 43 and 66 of the IT Act that are bail able and compoundable while offences under section 378 of the IPC are non-bail able and offences under section 425 of the IPC are non-compoundable. Further, in case of the offence of receipt of stolen property, the offence under section 66B of the IT Act is bail able while the offence under section 411 of the IPC is non-bail able. Similarly, in case of the offence of identity theft and cheating by personation, the offences under sections 66C and 66D of the IT Act are compoundable and bail able while the offences under sections 463, 465 and 468 of the IPC are non-compoundable and the offences under sections 468 and 420 of the IPC are non-bail able. Finally, in case of obscenity, the offences under sections 67, 67A and 67B of the IT Act are non-bail able while the offences under section 292 and 294 of the IPC are bail able. This issue has been dealt with by the Bombay High Court in the case of *Gagan Harsh Sharma v. The State of Maharashtra*[2] (discussed below) wherein offences under sections 408 and 420 of the IPC that are non-bail able and cannot be compounded other than with the permission of the court were in conflict with offences under sections 43, 65 and

66 of the IT Act that are bail able and compoundable.

AMENDMENT BROUGHT IN THE I. T. ACT BY AMENDMENT ACT OF 2008

Cyber Crime is a technology related offence. Technology is never static. It keeps on changing and getting better and better. At the same time Cyber Criminals are exploiting this advanced technology to discover sophisticated ways of committing crime. The Information Technology Act is the saviour in the nation to combat cyber crimes. Thus as the criminals are keeping pace with the advancement in technology, it is equally important for the Law to keep itself update with the recent trends in commission of crime and advancement in technology. With the same intention the Amendment Act of 2008 brought sweeping changes in the old IT Act. To overcome the lacuna of old I. T. Act, many bodies, teams of technical experts and advisory groups were construed. They studied the cyber legislations in other foreign countries and recent trend in cyber crime scenario. Their recommendations were scrutinized and the Parliament of India came up with Information Technology Amendment Act 2008. It was placed in the Parliament and passed without much debate. This Amendment Act got the nod of President 5 th February 2009. The Amendments were made effective on 27th October 2009.

Highlights of the Amendment Act, 2008

The newly amendment Act came with following highlights; It focuses on privacy issues.

- It focuses on Information Security.
- It came with surveillance on Cyber Cases.
- The Concept of Digital Signature was elaborated.
- It clarified reasonable security practices for corporate.
- Role of Intermediaries were focused.
- It came with the Indian Computer Emergency Response Team.
- New faces of Cyber Crime were added.

- Powers were given to Inspector to investigate cyber crimes as against only to DSP. Severe punishments and fine were added.

CONCLUSION

The Information Technology Act is the sole savior to combat cyber crime in nature. Though offences where computer is either tool or target also falls under the Indian Penal Code and other legislation of the Nation, but this Act is a special act to tackle the problem of Cyber Crime. As we already know for a fact that the IT Act, 2000 has an overriding effect over the IPC provisions while governing the cybercrimes, there are a lot of instances where IPC provisions are applied based on the subjective circumstances of every case. Though some people feel that IPC should not have a realm to govern cybercrimes, there are numerous cybercrimes that are not extensively dealt by the IT Act, 2000. Hence, after the due amendments are made to the IT Act which contains with respect to every cybercrime, then the IPC can be withdrawn from governing in the domain of cybercrimes.

ENDNOTES

[i] Jonathan clough, *Principles of Cybercrime* 12(Cambridge publication , 2ndedn 1998)
[ii] Petter Gottschalk, Policing *Cyber Crime* 75 (Lexis Nexis Publication , 2ndedn 2002)
[iii] Classification of cyber law, *available at*:https://www.scribd.com/doc/316141735/Characteristics-of-Cyber-Crime (last visited on 2ndnov. 2018)
[iv] Cyber Crime man's safety , *available at:* http://www.sbsnagarpolice.com/Cyber_crime.htm (last visited on 12 October 2018)
[v] supra note no 3
[vi] Nidhi Arya"Cyber Crime Scenario in India and Judicial Response" Published inInternational Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-4, June 2019,pp.1108-1112, URL:https://www.ijtsrd.com/papers/ijtsrd24
[vii] Ibid.
[viii] Raghav Punj, Cybercrime ,*available at*:https://www.interpol.int/Crimeareas/Cybercrime/Cybercrime (last visited on 18th October2018)
[ix] BLAPL No.7596 of 2016
[x] jud-917-wp-4361-2018
[xi] 2005 (3) ESC 1917