ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 6 Issue 2 March 2018

International Manuscript ID : 23482001V6I2032018-10

(Approved and Registered with Govt. of India)

Indian Penal Code, Legal Frameworks Towards Cyber Threats, Crimes and Offences

Dr. Gurmeet Singh

Associate Professor

Department of Law,

KGK College Moradabad. U.P.

Abstract

The introduction of the internet has brought the tremendous changes in our lives. People of all fields are increasingly using the computers to create, transmit and store information in the electronic form instead of the traditional papers, documents. Information stored in electronic forms has many advantages, it is cheaper, easier to store, easier to retrieve and for speedier to connection. Though it has many advantages, it has been misused by many people in order to gain themselves or for sake or otherwise to harm others. The high and speedier connectivity to the world from any place has developed many crimes and these increased offences led to the need of law for protection. Some countries have been rather been vigilant and formed some laws governing the net. In order to keep in pace with the changing generation, the Indian Parliament passed the law --- Information Technology Act 2000. The IT Act 2000 has been conceptualized on the United Nations Commissions on International Trade Law (UNCITRAL) Model Law. The increase rate of technology in computers has led to enactment of Information Technology Act 2000. The converting of the paper work into electronic records, the storage of the electronic data, has led tremendous changed the scenario of the country. The Act further amends the Indian Penal Code, 1860, The

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 6 Issue 2 March 2018

International Manuscript ID : 23482001V6I2032018-10

(Approved and Registered with Govt. of India)

Evidence Act, 1872, The Banker's Book's Evidence Act, 1891 and The Reserve Bank of India Act, 1934.

Keywords :Cyber Theats, Legal Framework with Cyber Crimes, I.T. Act of India

Introduction

Cybercrime is a generic term that refers to all criminal activities done using the medium of computers, the Internet, cyberspace and the worldwide web. Computer crime, or Cybercrime, refers to any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Netcrime is criminal exploitation of the Internet.

Classification of Cyber Offences

The increased rate of technology in computers has led to the enactment of Information Technology Act 2000. The converting of the paperwork into electronic records, the storage of the electronic data, has tremendously changed the scenario of the country.

Offenses: Cyber offenses are the unlawful acts which are carried in a very sophisticated manner in which either the computer is the tool or target or both. Cybercrime usually includes:

(a) Unauthorized access of the computers (b) Data diddling (c) Virus/worms attack (d) Theft of computer system (e) Hacking (f) Denial of attacks (g) Logic bombs (h) Trojan attacks (i) Internet time theft (j) Web jacking (k) Email bombing (l) Salami attacks (m) Physically damaging computer system.

The offenses included in the IT Act 2000 are as follows:

1. Tampering with the computer source documents.

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 6 Issue 2 March 2018

International Manuscript ID : 23482001V6I2032018-10

(Approved and Registered with Govt. of India)

2. Hacking with computer system.
3. Publishing of information which is obscene in electronic form.
4. Power of Controller to give directions
5. Directions of Controller to a subscriber to extend facilities to decrypt information
6. Protected system
7. Penalty for misrepresentation
8. Penalty for breach of confidentiality and privacy
9. Penalty for publishing Digital Signature Certificate false in certain particulars
10. Publication for fraudulent purpose
11. Act to apply for offense or contravention committed outside India
12. Confiscation
13. Penalties or confiscation not to interfere with other punishments.
14. Power to investigate offenses.

1. Tampering with computer source documents:

Section 65 of this Act 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 being time in force, shall be punishable with imprisonment up to three year, or with fine which may extend up to two lakh rupees, or with both.

Explanation:

For the purpose of this section “computer source code” means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 6 Issue 2 March 2018

International Manuscript ID : 23482001V6I2032018-10

(Approved and Registered with Govt. of India)

Many of the cyber-crimes penalised by the IPC and the IT Act have the same ingredients and even nomenclature. Here are a few examples:

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 lac) or both.

Section 378 of the IPC relating to "theft" of movable property will apply to the theft of any data, online or otherwise, since section 22 of the IPC states that the words "movable property" are intended to include corporeal property of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth. The maximum punishment for theft under section 378 of the IPC is imprisonment of up to 3 (three) years or a fine or both.

It may be argued that the word "corporeal" which means 'physical' or 'material' would exclude digital properties from the ambit of the aforesaid section 378 of the IPC. The counter argument would be that the drafters intended to cover properties of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth.

Section 424 of the IPC states that "*whoever dishonestly or fraudulently conceals or removes any property of himself or any other person, or dishonestly or fraudulently assists in the concealment or removal thereof, or dishonestly releases any demand or*

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 6 Issue 2 March 2018

International Manuscript ID : 23482001V6I2032018-10

(Approved and Registered with Govt. of India)

claim to which he is entitled, shall be punished with imprisonment of either description[1] for a term which may extend to 2 (two) years, or with fine, or with both." This aforementioned section will also apply to data theft. The maximum punishment under section 424 is imprisonment of up to 2 (two) years or a fine or both.

Section 425 of the IPC deals with mischief and states that "*whoever with intent to cause, or knowing that he is likely to cause, wrongful loss or damage to the public or to any person, causes the destruction of any property, or any such change in any property or in the situation thereof as destroys or diminishes its value or utility, or affects it injuriously, commits mischief*". Needless to say, damaging computer systems and even denying access to a computer system will fall within the aforesaid section 425 of the IPC. The maximum punishment for mischief as per section 426 of the IPC is imprisonment of up to 3 (three) months or a fine 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 lac) or both.

Section 411 of the IPC too prescribes punishment for dishonestly receiving stolen property and is worded in a manner that is almost identical to section 66B of the IT Act. The punishment under section 411 of the IPC is imprisonment of either description for a term of up to 3 (three) years, or with fine, or with both. Please note that the only difference in the prescribed punishments is that under the IPC, there is no maximum cap on the fine.

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 6 Issue 2 March 2018

International Manuscript ID : 23482001V6I2032018-10

(Approved and Registered with Govt. of India)

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 lac).

Section 419 of the IPC also prescribes punishment for 'cheating by personation' and provides that any person who cheats by personation shall be punished with imprisonment of either description for a term which may extend to 3 (three) years or with a fine or with both. A person is said to be guilty of 'cheating by personation' if such person cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is.

The provisions of sections 463, 465 and 468 of the IPC dealing with forgery and "forgery for the purpose of cheating", may also be applicable in a case of identity theft. Section 468 of the IPC prescribes punishment for forgery for the purpose of cheating and provides a punishment of imprisonment of either description for a term which may extend to 7 (seven) years and also a fine. Forgery has been defined in section 463 of

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 6 Issue 2 March 2018

International Manuscript ID : 23482001V6I2032018-10

(Approved and Registered with Govt. of India)

the IPC to mean the making of a false document or part thereof with the intent to cause damage or injury, to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed.

In this context, reference may also be made to section 420 of the IPC that provides that any person who cheats and thereby dishonestly induces the person deceived to deliver any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security shall be punished with imprisonment of either description for a term which may extend to 7 (seven) years, and shall also be liable to fine.

The only difference between the punishments prescribed under sections 66C and 66D of the IT Act and section 419 of the IPC is that there is no maximum cap on the fine prescribed under the IPC. However, the punishment under section 468 is much higher in that the imprisonment mat extend to 7 (seven) years. Further, whilst the IT Act contemplates both the imposition of a fine and imprisonment, the IPC uses the word 'or' indicating that the offence could be punished with imprisonment or by imposing a fine. Most importantly, the fundamental distinction between the IPC and the IT Act in relation to the offence of identity theft is that the latter requires the offence to be committed with the help of a computer resource.

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,

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 6 Issue 2 March 2018

International Manuscript ID : 23482001V6I2032018-10

(Approved and Registered with Govt. of India)

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 lac), 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 lac).

The provisions of sections 292 and 294 of the IPC would also be applicable for offences of the nature described under sections 67, 67A and 67B of the IT Act. Section 292 of the IPC provides that any person who, inter alia, sells, distributes, publicly exhibits or in any manner puts into circulation or has in his possession any obscene book, pamphlet, paper, drawing, painting, representation or figure or any other obscene object whatsoever shall be punishable on a first conviction with imprisonment of either description for a term which may extend to 2 (two) years, and with fine which may extend to Rs. 2,000 (Rupees two thousand) and, in the event of a second or subsequent conviction, with 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. 5,000 (Rupees five thousand).

Section 294 of the IPC provides that any person who, to the annoyance of others, does any obscene act in any public place, or sings, recites or utters any obscene song, ballad

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 6 Issue 2 March 2018

International Manuscript ID : 23482001V6I2032018-10

(Approved and Registered with Govt. of India)

or words, in or near any public place, shall be punished with imprisonment of either description for a term which may extend to 3 (three) months, or with fine, or with both.

Cyber-crimes not provided for in the IPC

The following cyber-crimes penalised by the IT Act do not have an equivalent in the IPC.

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 for which there is no equivalent provision in the IPC.

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.

To a certain extent, section 409 of the IPC overlaps with section 65 of the IT Act. Section 409 of the IPC provides that any person who is in any manner entrusted with property, or with any dominion over property in his capacity as a public servant or in the

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 6 Issue 2 March 2018

International Manuscript ID : 23482001V6I2032018-10

(Approved and Registered with Govt. of India)

way of his business as a banker, merchant, factor, broker, attorney or agent, commits criminal breach of trust in respect of that property, shall be punished with imprisonment for life or with imprisonment of either description for a term which may extend to 10 (ten) years, and shall also be liable to a fine. However, section 65 of the IT Act does not require that the person who tampers with or damages or destroys computer source documents should have been entrusted with such source code. Under section 409 of the IPC, criminal breach of trust should have been committed by someone to whom the property was entrusted.

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 lac) or with both.

There is no provision in the IPC that mirrors Section 66E of the IT Act, though sections 292 and 509 of the IPC do cover this offence partially.

Section 292 of the IPC has been discussed above. Section 509 of the IPC provides that if any person 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, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, such person shall be punished with simple imprisonment for a term which may extend to 1 (one) year, or with fine, or with both. Unlike section 66E of the IT Act which applies to victims of both genders, section 509 of the IPC applies only if the victim is a woman.

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 6 Issue 2 March 2018

International Manuscript ID : 23482001V6I2032018-10

(Approved and Registered with Govt. of India)

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. There is no corresponding provision in the IPC.

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

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 6 Issue 2 March 2018

International Manuscript ID : 23482001V6I2032018-10

(Approved and Registered with Govt. of India)

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.

Conclusion

When the IT Act was enacted, its focus was on putting in place technology law fundamentals like digital signatures, providing legal recognition for electronic documents and the like. Article 14 of the Constitution of India, 1950 ("Constitution") states that the State shall not deny to any person equality before the law or the equal protection of the laws within the territory of India. It is not our contention that the current state of affairs results in a per se violation of Article 14 of the Constitution even though it has created an unhappy state of affairs. The legislature does have the freedom to make specific laws for specific matters or situations. However, the docking of cyber-crimes in the IT Act does not appear to have been well thought through. Even though the IT Act penalised cyber-crimes with a broad brush through sections 43, 66 and 67, it was only in 2008 that the IT Act was amended[12] and provisions were made for specific cyber-crimes such as sending offensive messages through communication servers, dishonestly receiving a stolen computer resource or communication device, identity theft, violation of privacy, cyber terrorism etc. through sections 66A to 66F and sections 67A to 67C. These amendments stick out like an unwieldy appendage.

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 6 Issue 2 March 2018

International Manuscript ID : 23482001V6I2032018-10

(Approved and Registered with Govt. of India)

References

[1] Dennis Murphy (February 2010). "War is War? The utility of cyberspace operations in the contemporary operational environment" (PDF). Center for Strategic Leadership. Archived from the original (PDF) on 20 March 2012.

[2] Joseph, Aghatise E. (28 June 2006). "Cybercrime definition". www.crime-research.org.

[3] * Halder, D., & Jaishankar, K. (2011) Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9

[4] Wilbur, Kenneth C.; Zhu, Yi (24 October 2008). "Click Fraud". Marketing Science. 28 (2): 293–308. doi:10.1287/mksc.1080.0397. ISSN 0732-2399.

[5] Dashora, K. (2011). Cyber crime in the society: Problems and preventions. Journal of Alternative Perspectives in the social sciences, 3(1), 240-259.

[6] Aggarwal, P., Arora, P., & Ghai, R. (2014). Review on cyber crime and security. International Journal of Research in Engineering and Applied Sciences, 2(1), 48-51.

[7] Skibell, R. (2003). Cybercrime & (and) Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act. Berkeley Tech. LJ, 18, 909.

[8] Sabillon, R., Cano, J. J., Cavaller Reyes, V., & Serra Ruiz, J. (2016). Cybercrime and cybercriminals: A comprehensive study. International Journal of Computer Networks and Communications Security, 2016, 4 (6).

[9] Chung, W., Chen, H., Chang, W., & Chou, S. (2006). Fighting cybercrime: a review and the Taiwan experience. Decision Support Systems, 41(3), 669-682.

[10] Mayer, J. (2015). Cybercrime litigation. U. Pa. L. Rev., 164, 1453.