



ORIGINAL RESEARCH PAPER

Law

STATUTORY PROVISIONS FOR PREVENTION OF CYBER CRIMES UNDER THE INDIAN PENAL CODE – EXISTING LAW INSUFFICIENT?

KEY WORDS: Cyber crime, Information Technology Act, Indian Penal code, The offences and penalties.

Dr. Shashirekha Malagi

Assistant Professor of Law, Sir Siddappa Kambali Law College [Formerly University College of Law], Karnataka University, Dharwad, Karnataka. 580001.

ABSTRACT

Cyber crime has become a major area of concern across all the countries in the world, especially India. This is because of the government's active drive to achieve digital emancipation in a country where digital unawareness and low literacy are known to exist. This contrast between the state's aim and present circumstances is directly creating opportunities for cybercriminals. Though cybercrime has been developed based on the development of technology, but it is not much more different from conventional crimes. There was no statute in India for governing cyber crimes, involving privacy issues, jurisdiction issues, intellectual property rights issues and a number of other legal issues. With the tendency of misusing of technology, there arisen a need of strict statutory laws to regulate the criminal activities in the cyber space. The Information Technology Act, 2000 was enacted by Parliament of India to protect the field of e-commerce, e-governance, e-banking as well as penalties and punishments in the field of cyber crimes. But Information Technology Act, 2000 has not covered all the cybercrimes, IPC Act covers almost all the crimes and is applicable to Cyber crimes. Hence the law makers had amended IPC to cover all the cybercrimes and it is said as conventional Penal law in India. In light of the aforementioned significance, this article deals with the punishments available in the Indian Penal Code, 1860 for various cyber crimes apart from what was mentioned in the IT Act, 2000.

INTRODUCTION

Crime is a great hurdle in the development of a country and adversely affects the members of the society and lowers down the economic growth of the country. The Information Technology Act is a great savior to combat cyber crime. This Act is a special Act to tackle the problem of cyber crime though offences relating to computer also fall under the Indian Penal Code and other legislation in India. In India, criminal law means nothing but the 'Indian Penal Code (IPC)'. IPC deals with all kinds of offences and there are various criminal laws in India. IPC Act aims to cover all kinds of criminal offences which also include cybercrimes and offences. The Information and Technology Act has also recognized offences and crimes in India, but IPC covers all types of offences when compared to Information Technology Act, 2000. The Information Technology Act, 2000 and the Indian Penal Code, 1860 penalize a number of cyber-crimes and unsurprisingly, there are many provisions in the IPC and the IT Act that overlap with each other². This paper highlights the provisions of Information Technology Act, 2000 along with the sweeping changes brought in the Indian penal code.

Meaning of Cyber Crime

The Term 'Cyber Crime' needs no introduction in today's E-world. In this world, where everything is available at a click, crimes are also been committed at a click. Cyber Crime thus is the darker side of technology. It is a Crime where the computer is either a tool or a target³.

Hence Cyber Crime is a Computer related crime. The Information Technology Act, 2000 defines the terms access in computer network in section 2(a), computer in section 2(i), computer network in section (2j), data in section 2(0) and information in section 2(v). These are all the necessary ingredients that are useful to technically understand the concept of Cyber Crime. In a cyber crime, computer or the data are the target or the object of offence or a tool in committing some other offence. The definition of term computer elaborates that computer is not only the computer or laptop on our tables, as per the definition computer means any electronic, magnetic, optical or other high speed data processing devise of system which performs logical, arithmetic and memory function by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network. Thus the definition is much wider to include mobile phones, automatic washing machines, micro wave ovens etc⁴.

The cybercrime is also known as electronic crimes, computer-related crimes, e-crime, high technology crime, information age crime etc. In simple term we can describe "Cyber Crime" are the offences or crimes that takes place over electronic communications or information systems. These types of crimes are basically the illegal activities in which a computer and a network are involved. Due to the development of the internet, the volumes of the cybercrime activities are also increasing because when committing a crime there is no longer a need for the physical present of the criminal⁵.

Is Existing Law Insufficient?

The Information Technology Act, 2000 has been contentious legislation since its enactment. The Act gave a new direction to how cyber-crimes are dealt with in India. However, the question we ask today is whether it fits satisfactorily in the current scenario or does it require revision⁶. The Information Technology Act 2000 and Information Technology Amendment Act are though landmark first steps and became mile-stone in the technological growth of the nation; however the existing law is not sufficient. Many issues in cyber crime and many crimes are still left uncovered. Territorial Jurisdiction is a major issue which is not satisfactorily addressed in The Information Technology Act 2000 and Information Technology Amendment Act⁷. The Indian Penal Code is so well drafted that offences not listed in the Information Technology Act 2000 rightnow can still be tackled through it, till such time we are convinced that the Information Technology Act needs to be recast in order to cope with the expanding contours of Cybercrime⁸.

Parallel Provisions in the Indian Penal Code and Information Technology Act 2000

The Information Technology Act, 2000 extensively deals with numerous cybercrimes and their punishments. Along with this, the Indian Penal Code, 1860 also contains certain provisions which concern themselves with a number of cybercrimes. Many of the cyber-crimes penalised by the Indian Penal Code and the Information Technology Act have the same provisions and even nomenclature. Here are a few examples:⁹

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 lack) or both¹⁰.

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 earth¹¹.

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 claim to which he is entitled, shall be punished with imprisonment of either description¹ 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 both¹².

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 both¹³.

Receipt of stolen property:

Section 66B of the Information Technology 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 Information Technology Act is imprisonment of up to 3 (three) years or a fine of up to Rs. 1,00,000 (Rupees one lack) or both¹⁴.

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 fine¹⁵.

Identity theft and cheating by personation:

Section 66C of the Information Technology 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 lack).¹⁶

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 lack).¹⁷

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.¹⁸ 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 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.¹⁹

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.²⁰

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 may 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 resource²¹.

Obscenity:

Sections 67, 67A and 67B of the Information Technology 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 lack), 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 lack). 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 lakh) 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).²²

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 Information Technology 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 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.²³

Amendments to the IPC

The Indian legislature has from time to time, made a number of amendments to the IPC, to specifically cover cyber-crimes. The Indian Penal Code, 1860 got amended after enactment of Information Technology ACT 2000

The Indian Penal Code was amended by inserting the word 'electronic' thereby treating the electronic records and documents on a par with physical records and documents. The Sections dealing with false entry in a record or false document etc (e.g. 192, 204, 463, 464, 464, 468 to 470, 471, 474, 476 etc) have since been amended as 'electronic record and electronic document' thereby bringing within the ambit of IPC. Now, electronic record and electronic documents have been treated just like physical records and documents during commission of acts of forgery or falsification of physical records in a crime. After the above amendment, the investigating agencies file the cases/ charge-sheet quoting the relevant sections from IPC under section 463, 464, 468 and 469 read with the Information Technology Act under Sections 43 and 66 in like offences to ensure the evidence and/or punishment can be covered and proved under either of these or under both legislation.²⁴

Some of the important amendments are as follows:²⁵

- a. a new section 29A was created to define "electronic record" by linking it with the definition given in the Information Technology Act⁶;
- b. a new sub-section (3) was inserted in section 4 of the IPC (relating to the extension of the IPC to extra territorial offences) that states that the provisions of the IPC shall be applicable to any person in any place "without and beyond India", committing an offence targeting a computer resource located in India⁷;
- c. in sections 118 and 119 of the IPC (that deal with the concealment of a design to commit an offence punishable with death or imprisonment for life and a public servant concealing a design to commit an offence which it is his duty to prevent, respectively), the words "voluntarily conceals by any act or omission or by the use of encryption or any other information hiding tool, the existence of a design" were inserted before the words "to commit such offence or makes any representation which he knows to be false respecting such design"⁸; d. in section 464 of the IPC (which penalises the making of a false document), the

phrase "digital signature" was replaced with the phrase "electronic signature" in all places. The section was also amended to include the making of false electronic records and affixing electronic signatures under its ambit and the phrase "affixing electronic signature" was given the same meaning as it has under the IT Act⁹;

- e. "electronic record" was included within the ambit of sections 164, 172, 173, 175, 192, 204, 463, 466, 468, 469, 470, 471, 474 and 476 of the IPC that earlier only provided for "documents", "books", "paper", "writing" or "records", as the case may be;
- f. in section 466 of the IPC (which deals with forgery of court records or of public registers), the term "register" was defined to include any list, data or record of any entries maintained in an "electronic form", as defined in section 2(1) (r) of the IT Act¹⁰; and
- g. a new section 354D was inserted in the IPC that introduces the offence of cyber stalking, which has been discussed above.

CONCLUSION

The information and communication technology is the fast changing technology. We need to be updated with the development in the technology so we readily amend our existing laws to keep pace with the technology. This is the beginning of this technology, within two decades this technology has touched every individual life either directly or indirectly. It has its own advantages and disadvantages, and it has given birth to most deadliest of crime like cyber terrorism where in single click of a mouse it can kill thousands of people. There is an urgent need for unification of internet laws to reduce the confusion in their application. For e.g. for publication of harmful contents or such sites, we have Indian Penal Code (IPC), Obscenity Law, Communication Decency law, self regulation, Information Technology Act 2000, Data Protection Act, Criminal Procedure Code etc but as they deal with the subject vaguely therefore lacks efficient enforceability mechanism. Due to numerous Laws dealing with the subject there lays confusion as to their applicability, and none of the Law deals with the subject specifically in to. To end the confusion in applicability of Legislation picking from various laws to tackle the problem, there should be unification of laws by taking all the internet laws to arrive at Code which is efficient enough to deal with all the problems related to internet crimes.

REFERENCES

1. ² Cyber Security: A Legal Perspective, Dr. Sudhir Kumar Sharma, International Journal of Computer and Internet Security. ISSN 0974-2247 Volume 9, Number 1 (2017), pp. 1-11 © International Research Publication House <http://www.irphouse.com>
2. ³ Nikhil A. Gupta, CYBER CRIME AND INFORMATION TECHNOLOGY ACT 2000 - AN OVERVIEW ~, [http://mja.gov.in/Site/Upload/GR/Title %20NO.13\(As%20Per%20Workshop%20List%20title%20no13%20pdf\).pdf](http://mja.gov.in/Site/Upload/GR/Title%20NO.13(As%20Per%20Workshop%20List%20title%20no13%20pdf).pdf), (Visited on 16.3.2021)
3. ⁴ *Ibid*
4. ⁵ India: Cyber Crimes Under The IPC And IT Act - An Uneasy Co-Existence, <https://www.mondaq.com/india/it-and-internet/891738/cyber-crimes-under-the-ipc-and-it-act--an-uneasy-co-existence>.
5. ⁶ <https://criminallawstudiesnlj.wordpress.com/2020/06/02/section-67-of-it-act-2000-scope-misuse-and-the-striking-inadequacy/>, (Visited on 10.3.21)
6. ⁷ *Ibid*.
7. ⁸ Dr. Amita Verma, "Cyber Crimes and Law", 1st edn., (Allahabad: Central Law Publication, 2009), p.450
8. ⁹ <https://www.mondaq.com/india/it-and-internet/891738/cyber-crimes-under-the-ipc-and-it-act--an-uneasy-co-existence>
9. ¹⁰ *Ibid*.
10. ¹¹ Critical Analysis of Data Theft in Cyber Space, Shivani Johri,
11. ¹² <https://www.latestlaws.com/wp-content/uploads/2018/07/Critical-Analysis-of-Data-Theft-in-Cyber-Space-By-Shivani-Johri.pdf>, (Visited on 15.3.2021)
12. ¹³ <https://indiankanoon.org/doc/441951/>, (Visited on 15.3.2021)
13. ¹⁴ <https://indiankanoon.org/doc/48199014/>, (Visited on 15.3.2021)
14. ¹⁵ IPC Section 411. Dishonestly receiving stolen property, <https://www.latestlaws.com/bare-acts/central-acts-rules/ipc-section-411-dishonestly-receiving-stolen-property/>, (Visited on 15.3.2021)
15. ¹⁶ Cyber theft - A serious concern in India, <https://www.lexology.com/library/detail.aspx?g=4af6c044-dc77-4b1a-9288-986395eff8d1>, (Visited on 15.3.2021)
16. ¹⁷ Section 66D: Punishment for cheating by personation by using computer resource, <https://www.itlaw.in/section-66d-punishment-for-cheating-by-personation-by-using-computer-resource/>, (Visited on 14.3.2021)

17. ¹⁹ Anubhav Pandey, Cheating – Constituents, punishment and other legal issues related to cheating, <https://blog.ipleaders.in/cheating-constituents-punishment-legal-issues-related-cheating/>, (Visited on 15.3.2021)
18. ¹⁹ *Ibid*
19. ²⁰ *Ibid*
20. ²¹ <https://iritm.indianrailways.gov.in/uploads/files/1360312590693-12.Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf>
21. ²² Cyber Crimes, Ministry of Women and Child Development, <https://pib.gov.in/PressReleasePage.aspx?PRID=1602398>, (visited on 15.3.2021)
22. ²³ *Ibid*
23. ²⁴ An overview of cyber laws vs. cyber crimes: in Indian perspective, <https://www.lexology.com/library/detail.aspx?g=c0dd03b8-fab9-4daa-be5b-40b723537899>, (Visited on 3/3/2021)
24. ²⁵ Cyber Crimes Under The IPC And IT Act - An Uneasy Co-Existence, <https://www.mondaq.com/india/it-and-internet/891738/cyber-crimes-under-the-ipc-and-it-act--an-uneasy-co-existence>, (Visited on 6.3.2021)