CRITICAL ANALYSIS OF THE LAWS AGAINST CYBER-CRIMES IN INDIA

- RASIKA GUPTA

INTRODUCTION

The boom in globalisation coupled with computerisation in India has brought the dawn of several newer crimes in India. With the proliferation of internet dependency, these crimes are a juxtaposition of computers and the internet and are more specifically known as cyber-crimes.[1] Therefore, in the simplest terms, a cyber-crime can be defined as any such offense in which a computer is involved; when a computer or any information stored on it is the target, medium or the object of offense, it is recognized as a cyber-crime.[2]

A precise definition of "cyber-crime" is difficult owing to the fact that no Indian legislation: the Information Technology Act, 2000 ("**IT Act**"); the Information Technology Amendment Act, 2008 ("**ITA Act**"); Indian Penal Code, 1860 ("**IPC**") and the National Cyber Security Policy 2013 ("**Policy**") has ever defined it.

The tracing of cyber-crimes is exceptionally challenging owing to the virtual nature, anonymity and boundlessness of the cyber space. It accordingly requires an efficient regulatory framework. This is in the form of the aforementioned statutes that lay down offences under the purview of cyber-crimes and prescribe punishments for the same.

ANALYSIS OF GOVERNING LEGISLATIONS

With increase in the growth and development of information technology and the cyber world, cyber-crimes have also increased simultaneously. This was noted by the Courts,[3] since until 1999, the Indian legal system did not concern itself with any cyber law specially to control to

[1] A Bhatt, A Modern Law Library Action: The Future of Digital Books in Indian Law Schools. International Journal of Allied Practice, Research and Review, 5(1), pp.1-5 (2018).
[2] Sussman, 9 The critical challenges from international high-tech and computer-related crime at the millennium. Duke Journal of Comparative and International Law, 451-489 (1999).
[3] Sukanto Haldar v. State of West Bengal, AIR 1952 Cal 214; Jayesh S. Thakkar v. State of Maharashtra, WP No. 1611, Bombay HC, 2001; NASSCOM v. Ajay Sood, 2005 (30) PTC 437; State of Tamil Nadu v. Suhas Katti, decided by the Chief Metropolitan Magistrate, Egmore, on November 5, 2004; State of Punjab and Others v. M/s Amritsar Beverages Ltd., AIR 2006 SC 2820.

the criminal activity. The present cyber law of India is creation of the e-commerce, because the concept of corporate world has undergone change and the multinational companies are working and require the protection in the new modes of the business. New modes of communication utilized by the business community and the internet makes this a new threat to citizens.

Being a welfare state, it is duty of the state to protect the citizens in cyber-space as well. Therefore, legislative steps for regulating them led to the IT Act. This is in addition to the IPC that also deals with similar crimes. For instance, offences like hacking, data theft, virus attacks, denial of service attacks, illegal tampering with source codes including ransomware attacks could be prosecuted under Section 66 r/w S.43 of the IT Act. Cases of forging a credit or debit card or even cloning a mobile SIM with dishonest or fraudulent intent to cause wrongful loss or wrongful gain could be prosecuted under IPC provisions under Sections 463 to 471, as applicable. Cyber-crimes, that include offences like stalking and hawking, are also a violation of an individual's fundamental right of privacy.[4] In this regard, the following laws dealing with cyber-crimes are noteworthy to be analysed:

a. The Information Technology Act, 2000 And Information Technology Amendment Act, 2008:

The IT Act, based on the Model Law on e-commerce adopted by the United Nations Commission on International Trade Law in 1996 is the statute governing cyber law issues to protect the field of e-commerce, e-governance, e-banking in conjunction with providing penalties and punishments for cyber-crimes. Keeping in view several issues that crept in, it was amended by the ITA Act. Chapter XI defines certain offences and stipulates the punishments for such offences.

Section 65 deals with tampering in the form of concealing, destroying, altering with source documents, when the same is required to be maintained by law is an offence punishable with 3 years' imprisonment or Rs. 2 lakh or both. It attempts to thwart efforts to alter programs in such a way that they cannot be used by the person or institution who owns the program. This would

[4] Justice K. S. Puttaswamy (Retd.) and Anr. V. Union Of India And Ores, (2017) 10 SCC 1.

include fabrication of an electronic record or committing forgery by way of interpolations when produced as evidence.[5]

Similarly, Section 66 deals with the offence of unauthorised access to computer resource with dishonest intention in the form of data theft. It attracts imprisonment up to 3 years or a fine of Rs. 5 lakh or both. The ITA Act made this section more purposeful by removing the term "hacking" from the clause and widening the list of offences. It prohibits the sending offensive messages through electronic communication, sending emails to deceive the recipient, i.e., spoofing;[6] dishonestly receiving stolen a computer;[7] identity theft;[8] cheating by personation;[9] violation of privacy;[10] and cyber terrorism.[11] Each clause provides a corresponding penalty provision, especially the last which is relevant since it covers acts committed with intent to threaten the unity, integrity, security or sovereignty of India; consequently, punishment may extend to life.

For other offences mentioned in Section 66, punishment prescribed is generally up to 3 years and fine of up to Rs. 2 lakh has been prescribed and these offences are cognizable and bailable. Furthermore, as per Section 84B and 84C, abetment to commit an offence is made punishable with the fine and imprisonment up to one-half the longest term under the Act.

The IT Act also penalises the publishing or transmitting of obscene material in electronic form.[12] The ITA Act widened the ambit to include sexually explicit act in electronic form,[13] child pornography,[14] and retention of records by intermediaries.[15] The clause would accordingly include the screening of videographs and photographs of illegal activities, making pornographic video or MMS clippings or distributing such clippings through the Internet. It stipulates a first conviction for a term up to 3 years and fine of Rs. 5 lakh and second conviction for a term of 5

[5] Bhim Sen Garg v. State of Rajasthan, 2006 Cri LJ 3463.
[6] Section 66A, Information Technology Act, 2000.
[7] Section 66B, Information Technology Act, 2000.
[8] Section 66C, Information Technology Act, 2000.
[9] Section 66D, Information Technology Act, 2000.
[10] Section 66E, Information Technology Act, 2000.
[11] Section 66F, Information Technology Act, 2000.
[12] Section 67, Information Technology Act, 2000.
[13] Section 67A, Information Technology Act, 2000.
[14] Section 67B, Information Technology Act, 2000.
[15] Section 67C, Information Technology Act, 2000.

years and fine of Rs. 10 lakh or both. This section has historical importance since the first ever conviction under the IT Act was under it in *State of Tamil Nadu v. Suhas Katti*,[16] for cyber stalking and email spoofing.

With regards to child pornography,

With respect to child pornography, the law is very stringent. It is not only publishing or transmission of child porn that is an offence but even browsing for such content and retaining or downloading it is an offence too, unlike for pornography where only the dissemination and transmission, sale, etc. are considered offences. Further, actions intended to entice children through social media for creating child porn content or to record abuse of children and circulating the same are all offences punishable under the IT Act. Most offences carry maximum imprisonment of three years and fine. However, the more serious offences such as child pornography carry stronger punishment ranging from five to seven years. Crimes other than those affecting the "socio-economic conditions" or against women and children, may also be compounded.

The IT Act also empowers the Government or agencies as stipulated in the Section, to intercept, monitor or decrypt transmission of electronic message and communication if it is satisfied that it is necessary or expedient in the interest of sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence.[17] The ITA Act inserted Section 69A allowing for blocking for public access of any information under the aforementioned circumstances and Section 69B allows monitoring and collecting traffic data.

These newly inserted provisions are more intrusive and invasive than the erstwhile provision under the Indian Telegraph Act, 1885, since it allows the Government to listen in to all phone

[16] State of Tamil Nadu v. Suhas Katti, decided by the Chief Metropolitan Magistrate, Egmore, on November 5, 2004.
[17] Section 69, Information Technology Act, 2000.

calls, read SMSs and emails, and monitor the websites that one visited and has been criticised to be draconian, however the Supreme Court has upheld its constitutionality.[18]

The IT Act also applies to offences or contravention committed outside India, if the contravention or the offence involves a computer or a computer network located in India,[19] considering the global nature of cyber-crime.

b. The Indian Penal Code, 1860

Prior to the enactment of the IT Act, cyber crimes were governed by the IPC, being the conventional penal statute in India. It was amended by the IT Act to include offences involving electronic record.

Under Section 192, the meaning of fabricating false evidence has been amended to include any false entry or electronic records containing a false statement. This offence can be committed by using the computer as a tool. Additionally, crimes like web-jacking, sending threatening emails etc. are within the preview of Section 383 that deals with extortion. Cyber-crimes in the form of fraud, [20] and cheating,[21] also come under purview of IPC.

Additionally, cyber-crimes are made punishable under provisions such as Sections 119, 167, 173, 175, 405, 406, 463 and 465. As such, the launching of a computer virus also comes under the purview of IPC.[22] The Criminal Law Amendment Act 2013 inserted certain sections, which are covering the offences which are going to be committed by using the computer or any communication device. Special reference may be made to Section 354C, that deals with voyeurism, Section 354 which deals with stalking, that are now subjected to the internet and communication device. Stalking has been defined to include the monitoring of the use by a woman of the internet, email or any other form of electronic communication.[23] Also, cyber defamation is included in the purview of Section 499 when done with the help of computers or the Internet.

[18] Shreya Singhal v. Union of India, AIR 2015 SC 1523.
[19] Section 75, Information Technology Act, 2000.
[20] Section 25, Indian Penal Code, 1860.
[21] Section 415 and 416, Indian Penal Code, 1860.
[22] Section 425, Indian Penal Code, 1860.
[23] Section 354D, Indian Penal Code, 1860.

Despite the IT Act's existence, in practice, the investigating agencies often file cases quoting the relevant sections from IPC in addition to those corresponding in IT Act, such as under Sections 463, 464, 468 and 469 read with the IT Act or the ITA Act under Sections 43 and 66, to ensure the evidence or punishment stated at least in either of the legislations can be brought about easily.

c. The National Cyber Security Policy, 2013

Additionally, it may be noteworthy to mention the National Cyber Security Policy, 2013. With an aim to monitor and protect information and strengthen defences from cyber-attacks, the Policy was released by the Government of India. Its purpose is to ensure a secure and resilient cyber-space for citizens, businesses and the government. *Inter alia*, it adopts a suitable posturing to signal the resolve to make determined efforts to effectively monitor, deter & deal with cyber-crime and cyber-attacks. It seeks to reduce national vulnerability to cyber-attacks, preventing cyber-attacks and cyber-crimes, minimising response and recover time and effective cyber-crime investigation and prosecution. The policy also facilitates monitoring of key trends at the national level, including cyber-attacks and cyber-crime.[24]

d. Other Statutes

The IT Act also amended the Indian Evidence Act, 1872 giving recognition to all electronic records and documents as evidence. Additionally, it amended the Bankers' Books Evidence Act, 1891 to insert relevant provisions for the production of documents in electronic form. Also, the Copyright Act, 1957 also includes provisions for copyright infringement through electronic media,[25] and the knowing use of an infringing copy of a computer program to be an offence.[26] The Narcotic Drugs and Psychotropic Substances Act, 1985 penalises the online sale of drugs, and the Arms Act, 1958, bars the online sale of arms. These are noteworthy attempts to assist in curbing cyber-crimes in various areas of the law.

[24] Press Information Bureau, Ministry of Communications, Government of India, Shri Kapil Sibal releases National Cyber Security Policy, dated 2 July 2013, available at http://pib.nic.in/newsite/PrintRelease.aspx?relid=96971
[25] Section 51, Copyright Act, 1957.
[26] Section 63B, Copyright Act, 1957.

CONCLUSION

While the IT Act including its amending act is a thorough landmark first step and has become a milestone in the technological growth of the nation; however, the existing law does not suffice and many issues in cyber-crime are still left uncovered.

Several initiatives have been taken to ensure awareness among police and judiciary. These exercises have to be balanced with sensitisation programmes to ensure that the persons involved in the system understand the effects of cyber-crime and act expeditiously. There are, however, many old systemic problems. Also, there is rampant abuse and misuse of the provisions of the IT Act due to its opacity. Lack of awareness among users merely aggravates this problem.

Territorial jurisdiction is a major issue that has not been satisfactorily addressed and under Sections 46, 48, 57 and 61 in the context of adjudication process and the appellate procedure connected with and again in Section 80 and as part of the police officers' powers to enter, search a public place for a cyber-crime. Since the cyber-crime is geography-agnostic, borderless, territory-free and generally spread over territories of several jurisdiction; these issues are required to be addressed. Moreover, preservation of evidence is also big issue due to the easy manner in which evidence may be destroyed, such as on the intermediaries' computers. Furthermore, most cyber-crimes are still being brought under the relevant sections of IPC read with the comparative sections of IT Act, shows that convictions under the IT Act are proving to be difficult.

Another instance is of WhatsApp administrators being threatened with criminal prosecution for posts made in groups. Section 79, IT Act clearly exonerates persons who have no control over the content posted and the only liability is for complying with the intermediary rules. This would also apply to WhatsApp, the service provider, and not the person starting a group. This shows that an ambiguity is merely being misused in such instances.

Society continues to become more and more dependent upon technology and crime based on electronic offences are bound to increase.[27] An endeavour needs to be made to combat such

[27] Madon, and S Krishna, The Digital Challenge: Information Technology in the Development Context: Information Technology in the Development Context (2018).

offenders, through stringent rules and efficient convictions. The IT Act is a commendable piece of legislation, marking a landmark first step in the technological growth of the nation and must be used to its fullest extent.[28]

Expeditious action by police in clear cases of cyber-crime; collation of evidence in a manner that will withstand trial; and completion of court proceedings without delay with clear understanding of the technology and the law are just some goals that the system could aim for. It cannot ask users to "keep away" from use of technologies merely due to its inability to protect them. That is akin to asking women to not step out after dark.[29] Until the legal system demonstrates robustness, even irrespective of it, users must exercise due caution in the use of technology.[30] Adapt but do so with care and responsibility, as the virtual world requires as much caution as the real world.

REFERENCES

1. Ahmad, Tabrez, Challenges of Cyber Crimes in India: A Critical Analysis (May 12, 2018). 22nd World Multiconference on Systemics, Cybernetics and Informatics (WMSCI 2018) by International Institute of Informatics and Systemics, Orlando, Florida, USA, July 8-11, 2018. Available at SSRN: https://ssrn.com/abstract=3177396
2. Vakul Sharma, Information Technology Law and Practice- Cyber Laws and Laws Relating to E-Commerce (2018).
3. A Bhatt, A Modern Law Library Action: The Future of Digital Books in Indian Law Schools. International Journal of Allied Practice, Research and Review, 5(1), pp.1-5 (2018).
4. A Bajpai, Child rights in India: Law, policy, and Practice (2018).
5. Madon, and S Krishna, The Digital Challenge: Information Technology in the Development Context: Information Technology in the Development Context (2018).
6. Nandan Kamath, Law relating to Computers, Internet & E-commerce, Universal Publication, 5th Edition (2012).

[28] Nandan Kamath, Law relating to Computers, Internet & E-commerce, Universal Publication, 5th Edition (2012).
[29] NS Nappinai, ECONOMIC TIMES, Cyber Laws Part II: A guide for victims of cyber crime (2017), available at: //economictimes.indiatimes.com/articleshow/61464084.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
[30] Rodney D. Ryder, Guide to Cyber Laws (2003).

7. Yatindra Singh, Cyber Laws, 6th Edition (2016)
8. Damera Vijay Kumar, P S S Varma, and Shyam Sunder Pabboju, Security Issues in Social Networking, 13 IJCSNS International Journal of Computer Science and Network Security 6, (2013).
9. Abhishek Kumar, Subham Kumar Gupta, Animesh Kumar Rai, Sapna Sinha, 3 Social Networking Sites and Their Security Issues, International Journal of Scientific and Research Publications 4 (2013).
10. Laith T Khrais, 20 Highlighting the Vulnerabilities of Online Banking System, Journal of Internet Banking and Commerce 3 (2015).
11. Barkha U Rama Mohan, Cyber Law & Crime (2011).
12. Rodney D. Ryder, Guide to Cyber Laws (2003).
13. P.K. Singh, Laws on Cyber Crime (2007).