Legal Control Mechanism for Cyber Crime in India: A Critical Evaluation

Dr. Pawan Kumar, Mr.Ranjit Singh

Abstract- Information Technology has provided to us a new world of internet, business networking and e-banking, as a solution to reduce costs, change the sophisticated economic affairs to more easier, speedy, efficient, and time saving method of transactions. Internet has become a blessing for the present pace of life but at the same time it also gave a birth to various threats to the consumer, other institutions and departments. Various criminals like hackers, crackers have been able to establish a new way to interfere with the internet accounts through various techniques like hacking the Domain Name Server (DNS), Internet Provider's (IP) address, spoofing, phishing, internet phishing etc. This paper provides an understanding of the effects of misuse of Information technology, and how the present law in India is successful in dealing with the issue, and what way is the legal structure lagging to curb the crime. Possible changes needed in the system and the ways to combat cyber terrorism having safe and trustworthy transactions. There are many techniques that curb the criminal activities by cyber criminals but still the problem persists in legal structure and has failed to produce a deterring effect on the criminals. If the suggestions provided under the conclusion will be implemented then the national and international agencies in the field of prevention of cyber crime become more effective and they will easily curb the cyber crime and Information Technology Act 2000 will become more effective. It can still be held good for the objects it had existed to provide the benefits to the society. In this paper it is analyzed that public cannot gain adequate benefits from technology till the crime rate shall not be reduced.

I. INTRODUCTION

In India till 1999 there was no law for governing Cyber Laws involving privacy issues, jurisdiction issues, copyright issues, intellectual property rights issues and a number of other legal issues. There was no statute in India for governing Cyber Laws involving privacy issues, jurisdiction issues, intellectual property rights issues and a number of other legal questions. With the tendency of misusing of technology, there arisen a need of strict statutory laws to regulate the criminal activities in the cyber world and to protect the true sense of technology **"Information Technology Act, "**[1] 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. The above Act was further amended.[2] The ITA-2000 defines 'Computer' means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions 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. The word 'computer' and 'computer system' have been so widely defined and interpreted to mean any electronic device with data processing capability, performing computer functions like logical, arithmetic and memory functions with input, storage and output capabilities and therefore any high-end programmable gadgets like even a washing machine or switches and routers used in a network can all be brought under the definition.

II. MEANING OF CYBER CRIME

Cyber terrorists usually use the computer as a tool, target, or both for their unlawful act either to gain information which can result in heavy loss/damage to the owner of that intangible sensitive information. Internet is one of the means by which the offenders can gain such price sensitive information of companies, firms, individuals, banks, intellectual property crimes (such as stealing new product plans, its description, market programme plans, list of customers etc.), selling illegal articles, pornography etc. this is done through many methods such as phishing, spoofing, pharming, internet phising, wire transfer etc. and use it to their own advantage without the consent of the individual.

Many banks, financial institutions, investment houses, brokering firms etc. are being victimised and threatened by the cyber terrorists to pay extortion money to keep their sensitive information intact to avoid huge damages. And it's been reported that many institutions in US, Britain and Europe have secretly paid them to prevent huge meltdown or collapse of confidence among their consumers.

ENACTMENT OF INFORMATION TECHNOLOGY ACT, 2000

In India, the Information Technology Act, was enacted in 2000.[3] This was the first step to control and prevent cyber crime at national level. It was enacted taking into consideration UNICITRAL model of Law on e- commerce 1996. There are various provisions under the Information Technology Act, 2000 regarding control of cyber crime in India such as section 43 of this Act deals with Damage to Computer system etc. Section 66 provided compensation for Rupees 1crore for hacking intentionally and knowingly and fine will also imposed upto 2 lakh rupees, and imprisonment for 3 years.

This Act also provided for fine of 1 lakh rupees, and imprisonment of 5years, and double conviction on second offence if a person publish any obscene material in e-form. [4] Section72 deals with breaking confidentiality of the information of computer. Sec.73 deals with publishing of false digital signatures. Sec.74 Publication of Digital Signatures for fraudulent purpose. If a person committed any offence with regard to above sections then fine upto 2 lakh and imprisonment of 3 years and Imprisonment upto 10 years, fine upto 1 lakh and imprisonment upto 2 years, fine of 1 lakh, or imprisonment of 2 years or both and Imprisonment for the term of 2 years and fine for 1 lakh rupees shall be imposed respectively.

TYPES OF THREATS TO COMPUTER BY HACKERS

Hacker is computer expert who uses his knowledge to gain unauthorized access to the computer network. He's not any person who intends to break through the system but also includes one who has no intent to damage the system but intends to learn more by using one's computer. Information Technology Act 2000 doesn't make hacking per se an offence but looks into factor of mens rea. Crackers on other hand use the information cause disruption to the network for personal and political motives. Hacking by an insider or an employee is quite prominent in present date. Section 66 (b) of the Information Technology Act 2000, provides punishment of imprisonment for the term of 3 years and fine which may extent to two lakhs rupees, or with both.

Banks and other financial institutions are threatened by the terrorist groups to use their sensitive information resulting in heavy loss and in turn ask for ransom amount from them. There are various methods used by hackers to gain unauthorised access to the computers apart from use of viruses like Trojans and worms etc.

Therefore if anyone secures access to any computer without the permission of the owner shall be liable to pay damages of one crore rupees under Information Technology Act, 2000. Computer system here means a device including input and output support devices and systems which are capable of performing logical, arithmetical, data storage and retrieval, communication control and other functions but excludes calculators. Unauthorised access under Section 43 of the Information Technology Act 2000 is punishable regardless of the intention or purpose for which unauthorised access to the computer system was made. Owner needn't prove the facto of loss, but the fact of it been used without his authorisation.

Case of United States v. Rice would be important in this regard where defendant on the request of his friend (who was been under investigation by IRS officer) tried to find the status of his friend's case by using officer's computer without his consent. Though it didn't cause any damage/loss to the plaintiff (officer) but was convicted by the Jury for accessing the computer system of a Government without his authority and his conviction was later on confirmed. Even if one provides any assistance to the other to gain any unauthorised access to the computer he shall be liable to pay damages by way of compensation of Rupees 1 crore. Does turning on the computer leads to unauthorized access? The mens rea under section 1 of the Computer misuse Act, 1990 comprises of two elements there must be an intent to secure an access to any programme or data held in any computer, and the person must know that he intends to secure an unauthorized access. e.g. When defendants went to his former employee to purchase certain equipments and the sales person was not looking he was alleged to have keyed in certain commands to the computerized till granting himself substantial discount. Though section 1 (1) (a) requires "that second computer must be involved" but the judiciary in the case of R v. Sean Cropp, believed that the Parliament would have intended to restrict the offence even if single computer system was involved.

A) Computer Viruses:

Viruses are used by Hackers to infect the user's computer and damage data saved on the computer by use of "payload" in viruses which carries damaging code. Person would be liable under I.T Act only when the consent of the owner is not taken before inserting virus in his system. The contradiction here is that though certain viruses causes temporary interruption by showing messages on the screen of the user but still it's not punishable under Information Technology Act 2000 as it doesn't cause tangible damage. But, it must be made punishable as it would fall under the ambit of 'unauthorised access' though doesn't cause any damage. Harmless viruses would also fall under the expression used in the provision "to unsurp the normal operation of the computer, system or network". This ambiguity needs reconsideration.

B) Phishing:

By using e-mail messages which completely resembles the original mail messages of customers, hackers can ask for verification of certain information, like account numbers or

passwords etc. here customer might not have knowledge that the e-mail messages are deceiving and would fail to identify the originality of the messages, this results in huge financial loss when the hackers use that information for fraudulent acts like withdrawing money from customers account without him having knowledge of it

C) Spoofing:
This is carried on by use of deceiving Websites or e-mails. These sources mimic the original websites so well by use of logos, names, graphics and even the code of real bank's site.

D) Phone Phishing:
Is done by use of in-voice messages by the hackers where the customers are asked to reveal their account identification, and passwords to file a complaint for any problems regarding their accounts with banks etc.

E) Internet hacking:
Hacker here aims at redirecting the website used by the customer to another bogus website by hijacking the victim's DNS server[5] . This redirects user's original website to a false misleading website to gain unauthorised information.

F) Risk to Banks And Other Institutions:
Wire transfer is the way of transferring money from one account another or transferring cash at cash office. This is most convenient way of transfer of cash by customers and money laundering by cyber terrorists. There are many guidelines issued by Reserve Bank of India (RBI) in this regard, one of which is KYC (Know Your Customer) norms of 2002. Main objective of which is to:
1) Ensure appropriate customer identification, and
2) Monitor the transaction of suspicious nature and report it to appropriate authority every day bases.

G) Publishing obscenity material In Electronic Form:
Section 67 of the Information Technology Act, 2000 in parallel to Section 292 of Indian Penal Code, 1860 makes publication and transmission of any material in electronic that's lascivious or appeals to the prurient interest a crime, and punishable with imprisonment which may extend to 5 years and fine of 1 lakh rupees and subsequent offence with an imprisonment extending to 10 years and fine of 2 lakhs.
Various tests were laid down gradually in course of time to determine the actual crime in case of obscene material published in electronic form on net. Hicklin test was adopted in America in the case of Regina v. Hicklin wherein it was held that "if the material has tendency is to deprive and corrupt those whose minds are open to such immoral influences, and into whose hands a publication of this sort may fall". In Indian scenario the case of Ranjeet D. Udeshi v. State of Maharashtra[6] the Supreme Court admitted that Indian Penal Code doesn't define obscenity though it provides punishment for publication of obscene matter. There's very thin line existing between a material which could be called obscene and the one which is artistic.
Court even stressed on need to maintain balance between fundamental right of freedom of speech and expression and public decency and morality. If matter is likely to deprave and corrupt those minds which are open to influence to whim the material is likely to fall. Where both obscenity and artistic matter is so mixed up that obscenity falls into shadow as its insignificant then obscenity may be overlooked.
In the case of Miller v. California[7] it was held that local community standard must be applied at the time of determination of the offence. As it can traverse in many jurisdictions and can be accessed in any part of the globe. So wherever the material can be accessed the community standards of that country would be applicable to determine the offence of publication of obscene material posted in electronic form. Though knowledge of obscenity under Information Technology Act 2000 and Indian Penal Code may be taken as mitigating factor but doesn't take the case out of the provision.
This Act also provides punishment for an unauthorised access or, disclosure of that information to third person punishable with an imprisonment upto 2 years or fine which may extend to 1 lakh rupees or with both.[8] English courts have also dealt with an issue as to what activities would constitute crime under existing legislation, in the case of R. v. Fellows and Arnold[9] it was held that the legislation before the 1994 amendment would also enable computer data to be considered a 'copy of an indecent photograph' and making images available for downloading from the website would constitute material being 'distributed or shown'. Statute is wide enough to deal with the use of computer technology.

(H) Investment Newsletter:
We usually get newsletter providing us free information recommending that investment in which field would be profitable. These may sometimes be a fraud and may cause us huge loss if relied upon. False information can be spread by this method about any company and can cause huge inconvenience or loss through junk mails online.[10]

(I) Credit Card Fraud:
Huge loss may cause to the victim due to this kind of fraud. This is done by publishing false digital signatures. Most of the people lose credit cards on the way of delivery to the recipient or its damaged or defective, misrepresented etc.

MEASURES FOR PREVENTION OF CYBER CRIME

Though by passage of time and improvement in technology to provide easier and user friendly methods to the consumer for make up their daily activities, it has lead to harsh world of security threats at the same time by agencies like hackers, crackers etc. various Information technology methods have been introduced to curb such destructive activities to achieve the main objects of the technology to provide some sense of security to the users.

Few basic prominent measures used to curb cyber crimes are as follows:

A) Encryption: This is considered as an important tool for protecting data in transit. Plain text (readable) can be converted to cipher text (coded language) by this method and the recipient of the data can decrypt it by converting it into plain text again by using private key. This way except for the recipient whose possessor of private key to decrypt the data, no one can gain access to the sensitive information.

Not only the information in transit but also the information stored on computer can be protected by using Conventional cryptography method. Usual problem lies during the distribution of keys as anyone if overhears it or intercept it can make the whole object of encryption to standstill. Public key encryptograpy was one solution to this where the public key could be known to the whole world but the private key was only known to receiver, its very difficult to derive private key from public key.

B) Syncronised Passwords: These passwords are schemes used to change the password at user's and host token. The password on synchronised card changes every 30-60 seconds which only makes it valid for one time log-on session. Other useful methods introduced are signature, voice, fingerprint identification or retinal and biometric recognition etc. to impute passwords and pass phrases.[11]

C) Firewalls: It creates wall between the system and possible intruders to protect the classified documents from being leaked or accessed. It would only let the data to flow in computer which is recognised and verified by one's system. It only permits access to the system to ones already registered with the computer.

D) Digital Signature: Are created by using means of cryptography by applying algorithms. This has its prominent use in the business of banking where customer's signature is identified by using this method before banks enter into huge transactions.

INVESTIGATIONS AND SEARCH PROCEDURES

There are also provisions under the Information Technology Act, 2000 with regard to takes care of jurisdictional aspect of cyber crimes, and one would be punished irrespective of his nationality and place of commission of offence.[12] Power of investigation is been given to police officer not below the rank of Deputy Superintendent of police or any officer of the Central Government or a State Government authorised by Central Government. He may enter any public place, conduct a search and arrest without warrant person who is reasonably expected to have committed an offence or about to commit computer related crime. Accused has to be produced before magistrate within 24 hours of arrest. Provisions of Criminal Procedure Code, 1973 regulate the procedure of entry, search and arrest of the accused.

IMPEDIMENTS IN TRACKING OF OFFENCE

Most of the times the offenders commit crime and their identity is hard to be identified. Tracking cyber criminals requires a proper law enforcing agency through cyber border co-operation of governments, businesses and institutions of other countries. Most of the countries lack skilled law enforcement personnel to deal with computer and even broader Information technology related crimes. Usually law enforcement agencies also don't take crimes serious, they have no importance of enforcement of cyber crimes, and even if they undertake to investigate they are posed with limitation of extra-territorial nature of crimes.

CRITICAL ANALYSIS OF INFORMATION TECHNOLOGY ACT 2000

It can't be disputed that Information Technology Act, 2000 though provides certain kinds of protections but doesn't cover all the spheres of the I.T where the protection must be provided. Copyright and trade mark violations do occur on the net but Copy Right Act 1976, or Trade Mark Act 1999 are silent on that which specifically deals with the issue. Therefore have no enforcement machinery to ensure the protection of domain names on net. Transmission of e-cash and transactions online are not given protection under Negotiable Instrument Act, 1881. Online privacy is not protected only Section 43 (penalty for damage to computer or computer system) and 72 (Breach of confidentiality or privacy) talks about it in some extent but doesn't hinder the violations caused in the cyberspace.

Even the Internet Service Providers (ISP) who transmits some third party information without human intervention is not made liable under the Information Technology Act, 2000. One can easily take shelter under the exemption clause, if he proves that it was committed without his knowledge or he exercised due diligence to prevent the offence. It's hard to prove the commission of offence as the terms "due diligence" and "lack of knowledge" have not been defined anywhere in the Act. And unfortunately the Act doesn't mention how the extra territoriality would be enforced. This aspect is completely ignored by the Act, where it had come into existence to look into cyber crime which is on the face of it an international problem with no territorial boundaries.

III. CONCLUSION AND SUGGESTIONS

No one can deny the positive role of the cyber space in today's world either it be political, economic, or social sphere of life. But everything has its pro's and corns, cyber terrorists have taken over the technology to their advantage. To curb their activities, the Information Technology Act 2000 came into existence which is based on UNICITRAL model of Law on e-commerce. It has many advantages as it gave legal recognition to electronic records, transactions, authentication and certification of digital signatures, prevention of computer crimes etc. but at the same time is inflicted with various drawbacks also like it doesn't refer to the protection of Intellectual Property rights, domain name, cyber squatting etc. This inhibits the corporate bodies to invest in the Information technology infrastructure. Cases like Dawood and Quattrochi clearly reveals the problem of enforceability machinery in India. Cryptography is new phenomenon to secure sensitive information. There are very few companies in present date which have this technology. Other millions of them are still posed to the risk of cyber crimes.

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, Indian Penal Code, 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 toto. To end the confusion in applicability of Legislation picking from various laws to tackle the problem, it would suggest 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. Although these legislations talk about the problem but they don't provide an end to it. There's need for a one Cyber legislation which is co-ordinated to look after cyber crimes in all respects.With passage of time and betterment of technology in the present date, has also resulted in numerous number of Information technology related crimes therefore changes are suggested to combat the problem equally fast.

Crucial aspect of problem faced in combating crime is that, most of the countries lack enforcement agencies to combat crime relating to internet and bring some level of confidence in users. Present law lacks teeth to deter the terrorist groups for committing cyber crimes if you see the punishment provides by the Act it's almost ineffective, inefficient and only provides punishment of 3 years at the maximum. Harsher laws are required at this alarming situation to deal with criminals posing threat to security of funds, information, destruction of computer systems etc.Data protection, by promotion of general principles of good information practice with an independent supervisory regime, would enable the law to maintain sufficient flexibility to achieve an appropriate balance between the need to protect the rights of the individuals and to have a control over the way their personal information have been used would be helpful in this increasingly networked economy. Just having two provisions in the Information Technology Act, 2000 for protection of data without any proper mechanism for to tackle the crime makes their mention in the Act redundant.

Information Technology Act is applicable to all the persons irrespective of their nationalities (i.e. to non-citizens also) who commits offence under the Information Technology Act outside India, provided the act or conduct constituting the offence or contravention involves computer, computer systems, or computer networks located in India under Section 1 and Section 75 of the Information Technology Act, but this provision lacks practical value until and unless the person can be extradited to India. Therefore it's advised that we should have Extradition treaties among countries. To make such provisions workable.

It's like 'eye for an eye' kind of situation where the technology can be curbed only by an understanding of the technology taken over by cyber criminals. Even if the technology is made better enough to curb the computer related crime there is no guarantee if that would stay out of reach of cyber terrorists. Therefore Nations need to update the Law whether by amendments or by adopting sui generic system. Though Judiciary continues to comprehend the nature of computer related crimes there is a strong need to have better law enforcement mechanism to make the system workable.

IV. REFERENCES

[1]. Sankar Sen, 'Human Rights & Law Enforcement', 1st ed., 2002, Concept Publishing Co., New Delhi.
[2]. Dr. Sub hash Chandra Gupta, 'Information technology Act, 2000 and its Drawbacks', National Conference on Cyber Laws & Legal Education, Dec. 22-24th 2001, NALSAR, University of Law, Print House, Hyderabad.
[3]. Dr. Farooq Ahmed, 'Cyber Law in India (Laws on Internet)', Pioneer Books, Delhi.

[4]. 1992 U.S. App. LEXIS 9562 (4th May 4, 1992)
[5]. Dr. Farooq Ahmed, 'Cyber Law in India (Laws on Internet)', Pioneer Books, Delhi.
[6]. R v. Sean Cropp, Snearesbrook Crown Court, 4th July 1991. (303)
[7]. B.R Suri & T.N Chhabra, 'Cyber Crime', 1st ed., 2002, Pentagon Press, Delhi.
[8]. Dr. Farooq Ahmed, 'Cyber Law in India (Laws on Internet)', Pioneer Books, Delhi.
[9]. Rupam Banerjee, 'The Dark world of Cyber Crime', July 7, 2006 can be viewed at http://articles.sakshay.in/index.php?article=15257
[10]. Prof. Unni, 'Legal Regulations on Internet Banking', 2007, NALSAR University of Law, Hyderabad.
[11]. "Anusuya Sadhu", "The Menace of Cyber Crime", can be viewed at http://www.legalserviceindia.com/articles/article+2302682a.htm
3 L.R.Q.B. 360, 371 (Q.B. 1868).
AIR 1965 SC 881.
413 U.S 15.24 (1973)
[12]. Dr. Farooq Ahmed, 'Cyber Law in India (Laws on Internet)', Pioneer Books, Delhi.
[13]. B.R Suri & T.N Chhabra, 'Cyber Crime', 1st ed., 2002, Pentagon Press, Delhi.
[1997] 2 All ER 548
[14]. Justice S.B. Sinha, 'Cyber Crime in the Information Age', National Conference on Cyber Laws & Legal Education, Dec. 22-24th 2001, NALSAR, University of Law, Print House, Hyderabad.
[15]. Prof. V.K Unni, 'Legal strategies for a Robust I.T Infrastructure', 2007, NALSAR University of Law Hyderabad.
[16]. Dr. Farooq Ahmed, 'Cyber Law in India (Laws on Internet)', Pioneer Books, Delhi.
[17]. Sanker Sen, 'Human Rights & Law Enforcement', 1st ed., 2002, Concept Publications, New Delhi.
[18]. Dr. Farooq Ahmed, 'Cyber Law in India (Laws on Internet)', Pioneer Books, Delhi.
[19]. Ajmal Eddappagath, 'Cyber Laws and Enforcement'
[20]. Can be viewed at http://www.iimahd.ernet.in/egov/ifip/dec2004/article2.htm
[21]. Dr. Subhash Chandra Gupta - Information Technology Act, 2000 and its drawbacks, 'National Conference on Cyber Laws & Legal Education', Dec. 22-24th 2001, NALSAR, University of Law, Print House, Hyderabad.
[22]. C. Suman and Duvva Pavan Kumar, 'Data Protection - An overview', National Conference on Cyber Laws & Legal Education, Dec. 22-24th 2001, NALSAR, University of Law, Print House, Hyderabad.
[23]. Cris Reed and John Angel, 'Computer Law', 5th ed., 2003, Oxford University Press Inc., New York.
[24]. S.K Verma and Raman Mittal, 'Legal Dimensions of Cyber Space, 2004, Indian Law Institute, New Delhi.
[25]. Cris Reed and John Angel, 'Computer Law', 5th ed., 2003, Oxford University Press Inc. New York.