Cyber Law in Developing Countries: An Indian Perspective

Author
Dr. Swarupa N. Dholam

Institution
Bombay High Court, Mumbai, Maharashtra, India

Abstract - This paper provides a comprehensive overview of the relevant topics linked to the various aspects of cyber crime and focuses on the circumstances in India as developing countries. The paper contains four main topics. After an introduction (1st topic), it provides an overview of the phenomena of cyber crime and its causes (2nd topic). It followed descriptions of kinds of cyber crimes are committed in India and explanations as to why they have might be committed. An overview of the legal instruments over cyber crime is also provided in it (3rd topic). It continues with an analysis of different case laws with regard to cyber crime, its procedural law, digital evidence (4th topic).

Categories and Subject Descriptors

K.5.2 [Legal Aspects of Computing]: Cyber law in developing countries

General Terms

Cyber Law, Cyber Crime

Keywords

Cyber Stalking, Cyber hacking, Cyber Fraud, Cyber Pornography, Cyber Defamation, Software piracy, Cyber Terrorism, Cyber Phishing, Email Spoofing

1. INTRODUCTION

Countries are divided into two major categories by the United Nations, which are developed countries and developing countries. The classification of countries as a Developed and Developing country is based on economic status like GDP, GNP, per capita income, industrialization, standard of living, etc. Developed Countries is a country which provide free, healthy and secured atmosphere to live but the countries which lacks the same is known as Developing Countries.

United Nations Statistics Division claims that "There is no established convention for the designation of 'developed' and 'developing' countries or areas in the United Nations system. The designations 'developed' and 'developing' are intended for statistical convenience and do not necessarily express a judgment about the stage reached by a particular country or area in the development process". [1]

The computer technology currently in use is basically the same around the world. Apart from language issues and power adapters, there is very little difference between the computer systems and cell phones sold in Asia and those sold in Europe. An analogous situation arises in relation to the Internet. Due to standardization, the network protocols used in countries on the African continent are the same as those used in the United States. Standardization enables users around the world to access the same services over the Internet.

Finding response strategies and solutions to the threat of cyber crime is a major challenge, especially for developing countries. A comprehensive anti-cyber crime strategy generally contains technical protection measures, as well as legal instruments. The development and implementation of these instruments need time. Technical protection measures are especially cost-intensive.

The risks associated with weak protection measures could in fact affect developing countries more intensely, due to their less strict safeguards and protection. The ability to protect customers, as well as firms, is a fundamental requirement not only for regular businesses, but also for online or Internet-based businesses. In the absence of Internet security, developing countries could encounter significant difficulties promoting e-business and participating in online

service industries. The development of technical measures to promote cyber security and proper cyber crime legislation is vital for both developed countries and developing countries.

2. CAUSE OF CYBER CRIME IN INDIA

The motivating factors that encourages or drive individuals into cyber crime varies and it is determined based on a number of different factors such as money / financial gain, recognition / fame, low rate of conviction or even being caught, easy to perpetrate, intellectual pursuit, frustration, revenge etc. Below are the important factors.

2.1 Reliance on Information Communication Technologies (ICTs)

Many everyday communications depend on ICTs and Internet-based services, including VoIP calls or email communications. ICTs are now responsible for the control and management functions in buildings, cars and aviation services. The further integration of ICTs into everyday life is likely to continue. Short interruptions to services could cause huge financial damages to e-commerce businesses. The dependence of society on ICTs is not limited to the western countries. Developing countries also face challenges in preventing attacks against their infrastructure and users.

2.2 Number of users

The popularity of the Internet and its services is growing fast. Computer companies and Internet Service Providers (ISPs) are focusing on developing countries with the greatest potential for further growth. Development of cheap hardware and wireless access will enable even more people to access the Internet. With the growing number of people connected to the Internet, the number of targets and offenders increases.

2.3 Availability of devices and access

Only basic equipment hardware, software and Internet access are needed to commit computer crimes. Criminals can commit serious computer crimes with only

cheap or second-hand computer technology – knowledge counts for far more than equipment. The last vital element is Internet access. Although the cost of Internet access is higher in most developing countries than in industrialized countries, the number of Internet users in developing countries is growing rapidly. Offenders will generally not subscribe to an Internet service to limit their chances of being identified, but prefer services they can use without registration. The most common methods criminals can use to access the network fairly anonymously are public Internet terminals, open wireless networks, hacked networks and prepaid services without registration requirements. [2]

2.4 Availability of information

The Internet has millions of web pages of up-to-date information. [3] Anyone who publishes or maintains a web page can participate. One example of the success of user-generated platforms is Wikipedia, an online encyclopedia where anybody can publish. The success of the Internet also depends on powerful search engines that enable users to search millions of web pages in seconds. This technology can be used for both legitimate and criminal purposes.

2.5 Missing mechanisms of control

All mass communication networks from phone networks used for voice phone calls to the Internet; need central administration and technical standards to ensure operability. The Internet also needs to be governed by laws, and lawmakers and law-enforcement agencies have started to develop legal standards necessitating a certain degree of central control.

3. CYBER CRIME AND ITS VARIOUS KINDS IN INDIA

The term 'Cyber Crime' is frequently used in 21st century knowledge society and is created by combination of two words 'cyber' and 'crime'. The term 'cyber' denotes the cyberspace i.e. virtual space and means the informational space modeled through computer, in which various objects or symbol images of information exist. It is the place where the computer programs work and data is processed. However, the term 'crime' refers to a social and economic phenomenon and is as old as the

human society. Crime is a legal wrong that can be followed by criminal proceedings which may result into punishments. [4]

3.1 Cyber Hacking

In the globalized, liberalized era of communication convergence and new technology, the server is in one State and user in other State. The application of law in cyberspace is very complex due to undefined Jurisdiction. It is international as well as national legal challenge. India enacted the Information Technology Act, 2000 following the United Nation's Model Law, 1997. The Information Technology Act, 2000 specifically Section 43 and 66 deals with hacking and unauthorized access to computer, computer system and computer network. Cyber hacking does not mean no loss to human life because hackers are human being and they are causing injury to human society.

3.1.1

After the Pokhran test in June 1998, a group of international hackers, calling themselves Milworm, hacked the Website of India's Bhabha Atomic Research Center (BARC) and put up a spoofed Web page showing a mushroom cloud and the text "If a nuclear war does start, you will be the first to scream". The hackers were protesting India's nuclear weapons tests, although they admitted they did it mostly for thrills. They said that they also download several thousand pages of e-mail and research documents, including messages between India's nuclear scientists and Israeli Government officials, and had erased data on two of BARC's servers. [5]

3.1.2

On 5th July 2001 the Cyber Crimes Investigation Cell Mumbai received an unknown telephone that their website www.ccicmumbai.com is going to be attacked by hackers. Immediately Police Officers noticed that it has been hacked. They identified the hackers who replaced the original homepage of the Mumbai Police website and posted there obscene comments and abuses to Police Officials. The Police Officers investigated that Internet Protocol address which was related to this hacking belonged to the internet provider company DISHNET SSL LTD,

Mumbai and the end user of that same date and time was identified by internet provider immediately. After investigation the police arrested Anand Ashok Khare and Mahesh Mhatre for committing hacking. Both accepted their guilt and are now working with Mumbai Police Cyber Crime Investigation Cell for the prevention and control of hacking under assumed identities as 'Dr. Neruker' and 'Dr. Libran' respectively. [6]

3.2 Cyber Fraud

The term "cyber fraud" is not defined in the IT Act, 2000 in India. However, according to D. Bainbridge, the phrase 'Computer fraud' is used to describe 'stealing money or property by means of a computer that is using a computer to obtain dishonestly, property including money and cheques, credit card services, or to evade dishonestly some debt or liability. It might involve dishonestly giving an instruction to a computer to transfer funds into a bank account or using a forged bank card to obtain money from a cash dispenser i.e., automated teller machine. [7]

The Audit Commission of the United Kingdom (UK) defined 'cyber fraud' as 'any fraudulent behaviour connected with computerization by which someone intends to gain financial advantage'. [8]

Several provisions of the IPC, 1860 are relevant which prohibit and prescribe punishment for fraudulent activities. The IPC has been amended to give effect to the IT Act, 2000, specially provisions relating to cheating and dishonestly inducing delivery of property or valuable security, forgery, punishment for forgery, forgery of valuable security, using as genuine a forged document etc.

3.2.1

Mr. C. Suresh, the Managing Director of Vinsri InfoTech and owner of the website InfoTech Pvt. Ltd. had started his business in 1997 of data conversion, to give data entry works, to provide services for data entry, medical transcription, management and e-Books etc. In January 2002, he fraudulently received Rs. 2.5 lakh non-refundable deposits from each of the clients giving false promise to give data entry work. And in February 2003, when cheques issued to his clients by him

were not cleared rather dishonored because funds were not available; his clients started demanding either refund of their deposited amount or clearance of their bills and to provide work. But Mr. C. Suresh, the accused was silent. Therefore, his clients went to police and lodged separate complaints. Then he was arrested from Secundrabad on the charge of cyber fraud i.e. about Rs. 20 crore data conversion fraud. [9]

3.3 Cyber Pornography

Morality has sociological and psychological aspects. Morality is individual's perception due to which human beings accept certain things as good and reject certain things as bad in society. It varies from person to person and society to society. What is immoral for one is not so to other or in other society. There is no yardstick to determine what things are moral and what are immoral. Therefore, it is left to the judiciary as reasonable and prudent repository of moral standard in society. Law and morality are closely related. When there is synthesis between them in society, there will be no conflict and society will progress smoothly and fast. But all morals are not enforceable by law rather we have to make a balance and accept shared morality. [10]

The Indian Penal Code, 1860 and The Information Technology Act, 2000 provides limitations and prohibitions of certain things which are obscene. It prohibits sale, distribution, publication, export, import etc. of obscene books, pamphlets, papers, writings, drawings, paintings, representations and the like except justifications like literature, art, learning, monuments, etc. and prescribes punishments. It prohibits sale of obscene objects to young persons and obscene acts and songs to annoyance of others in or near any public place and prescribes punishments. It also prohibits word, gesture or act intended to insult the modesty of a woman. Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.

3.3.1

Tamil Nadu v. Suhas Katti, [11] was the first case of the Cyber Crime Cell Chennai. The defendant was charged for annoying, obscene and defamatory message in the yahoo message group relating to a divorce woman. The accused at first opened a false account in the name of the victim and then sent her information through e-mails. It annoyed the victim because she had to face harrowing calls. The victim filed a complaint about the fact before police. The Chennai police traced the accused at Mumbai and arrested him immediately after few days. On the basis of the expert witness the court held that the crime is conclusively proved and the accused was convicted and sentenced to undergo rigorous imprisonment for 2 years and to pay Rs. 500 fine u/s 469 of the IPC i.e. forgery for the purpose of harming reputation; for the offence u/s 509 of the IPC i.e. word, gesture or act intended to insult the modesty of a woman with 1 year simple imprisonment and Rs. 500 fine; and for the offence u/s 67 of the IT Act, 2000 with 2 years rigorous imprisonment and Rs. 4000 fine. The court held that all these sentences must run concurrently.

3.3.2

A Delhi Public School boy allegedly filmed his girlfriend in an act of oral sex with him on his cell phone camera which is to be called as MMS clip. This video clip was then forwarded by him to his friends, and then his friends sent it to others. Gradually, within a minute it was available to almost all users and even it was available for small price to the roadside vendors. The clip was copied to VCD (Video Compact Disk) for sale and distribution. One IIT Kharagpur student named Ravi Raj put that MMS clip of 2.37 minutes for auction on the Baazee.com which was India's top auction website and owned by e-Bay. The Delhi police arrested DPS student, Mr. Ravi Ray Singh and the portal's CEO, Mr. Avnish Bajaj. The counsel for the boy contended that the charge against his client is totally false and it is very difficult to prove who was that particular person because there was no visual of his face in the clip and he prayed for bail u/s 12 of the Juvenile Justice Act, 2000 though he was arrested u/s 293, 294, 201 of the IPC, 1860 and Section 67 of the IT Act, 2000. [12]

New multimedia technology is being misused and abused by criminals in cyberspace. Cyber pornography, online child pornography, cyber spamming etc. are increasing every moment. Cyber pornography is not only national but also international legal challenge which needs intensive study, research and world-wide awareness.

3.4 Cyber Stalking

The 'Web' is no more and no less than a mirror of the real world, and that means it also contains electronic versions of real life problems. Stalking is a problem that many people especially women, are familiar with in real life. These problems can occur on the internet as well, what has become known as 'Cyber Stalking' or 'on-line harassment'. It does not end here there have been many examples of cyber stalking crossing over to real life stalking where even physical danger is of high probability. [13]

3.4.1

The Delhi Police has registered India's First Case of Cyberstalking in 2001 where a lady named Ritu Kohli complained that a person who was using her identity to chat over the Internet at the website www.mirc.com was also deliberately giving her telephone number to other chatters encouraging them to call Ritu Kohli at odd hours. As a result of which, Mrs. Kohli received an estimate of 40 calls, national as well as international, during odd hours within 3 days. A case was registered under section 509 of the Indian Penal Code.

3.5 Cyber Defamation

In India, issue of defamation has so far been dealt under the provisions [Ss.499-502] of the Indian Penal Code, 1860. The Code makes no distinction between a slander and a libel. The Information Technology Act, 2000 provides for punishment to whoever transmits or publishes or causes to be published or transmitted, any material which is obscene in electronic form with imprisonment.

A claim for damage to reputation will warrant an award of damages only if the plaintiff has a reputation in the place where the publication is made. This has always

been the accepted legal principle in the common law countries. In India, the same principal has been adopted-publication takes place when and where the contents of the publication, oral, spoken or written are seen and heard, and comprehended by the reader or hearer.

3.5.1

In the first case of cyber defamation in India, SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra, the reputation of a corporate was being defamed by an employee of the plaintiff company by sending derogatory, defamatory, obscene, emails obscene, vulgar, filthy and abusive emails to its employers and also to different subsidiaries of the said company all over the world with the aim to defame the company and its Managing Director. The Hon'ble Judge of the Delhi High Court passed an ex-prate ad interim injunction observing that a prima facie case had been made out by the plaintiff. Consequently, the Delhi High Court restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails either to the plaintiffs or to its sister subsidiaries all over the world including their Managing Directors and their Sales and Marketing departments. Further, Hon'ble Judge also restrained the defendant from publishing, transmitting or causing to be published any information in the actual world as also in cyberspace which is derogatory or defamatory or abusive of the plaintiffs. [14]

3.5.2

In the case of Tata Sons vs. Turtle International, [15] the Delhi High Court has held that publication is a comprehensive term, embracing all forms and mediums – including the Internet. That an internet publication has wider viewership, or a degree of permanence, and greater accessibility, than other fixed (as opposed to intangible) mediums of expression does not alter the essential part, i.e. that it is a forum or medium. There is much sense to have more defined criteria taking into account the nature of the internet content. Injunctions on internet content should not be readily granted (especially ex-parte) since, firstly the internet is an easy, self-publishing platform providing a medium of expression for marginal individuals not having corporatist outlets. Secondly, the internet facilitates the distribution of

content for a minor cost to a vast audience. Both the alleged injury and the free speech concern are greater due to the wider dissemination of the content. These are only some concerns which set the internet apart and it is desirable to have a nuanced appreciation.

3.6 Software Piracy

Unauthorized copying of some purchased software. Most software programs purchased are licensed for use by just one user or at just one computer site. Moreover, when someone buys software, he or she is known as a "licensed user" rather than as an owner of the software. As a licensed user, an individual is permitted to make copies of the software program for back-up purposes only. [16] In India, the copyright of computer software is protected under the Indian Copyright Act of 1957.

3.7 Cyber Terrorism

There are two prime concepts of Cyber Terrorism –

1) When terrorists use information technology to attract their audience by creating violence, through defacement of web site, denial of service attack, hacking, cracking, tampering source code, flowing viruses etc. where computer is used a target or weapon and which go against Government or national security,

2) Another is terrorized use of IT i.e. cyber pornography, cyber fraud, cyber theft, spamming etc. which causes terror or threat in the mind of people. [17]

Internet has no boundary and it is not possible to define definite jurisdiction in cyber space. Therefore, terrorist groups are increasing day by day and they can easily access one another even living in different countries. Nowadays most of the terrorist groups have their own websites or information way.

Information and Communication Technology are very much used by terrorists in India for attack against the nation. Telephone, mobile phone, wireless, computer

facilities are available almost everywhere in India. That is why terrorists are able to communicate with each other even being in remote rural area. They can control the entire group activities from remote areas.

3.8 Cyber Phishing

Phishing is a fraudulent attempt, usually made through emails, SMS, phone call, etc. to seeking your personal information. Criminal sends false links and creates a "mirror" website that look like a legitimate website for trapping this crime. The fake website will fool people and taking into the criminal's site and collect your valuable information like your user name and password. Sec. 420, 464 Indian Penal Code & Sec. 66 D of IT Act are dealt with such kind of offences.

3.8.1

One financial Institute registered a crime stating that some persons ("perpetrators") have perpetrated certain acts through misleading emails ostensibly emanating from ICICI Bank's email ID. Such acts have been perpetrated with an intent to defraud the Customers. The Investigation was carried out with help of those emails received by the customers of that financial Institute and arrested the accused, the place of offence at Vijaywada was searched for the evidence. There one Lap Top and Mobile Phone was seized which was used for the commission of the crime. The arrested accused had used open source code email application software for sending spam emails. He has down loaded the same software from net and then used it as it is. The financial Institute customers those who have received his email felt that the email was originated from the financial Institute bank. When they filled the confidential information and submitted that time said information was directed to accused. This was possible because the dynamic link was given in the first page (Home page) of the fake website. The dynamic link means when people click on the link provided in spamming email that time only the link will be activated. The dynamic link was coded by handling the Internet Explorer on click event and the information of the form will be submitted to the web server (Where the fake website is hosted). Then server will send he data to configured email address and in this case email configured was to the accused email. So on

submission of the confidential information the information was directed to email ID accused email .The all the information after fishing (user name, password, Transaction password, Debit card Number and PIN, mother's maiden name) which he had received through Wi-Fi internet connectivity of Reliance.com which was available on his Acer Lap Top. [18]

3.9 Email Spoofing

E-mail spoofing is the forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source. A spoofed email is one that appears to originate from one source but actually has been sent from another source. Sec. 463, 464, 468, 489 of Indian Penal Code and Sec. 66-D of IT Act.

4. CONCLUSION

A legal framework for the cyber world was conceived in India in the form of E-Commerce Act, 1998. Afterwards, the basic law for the cyberspace transactions in India has emerged in the form of the Information Technology Act, 2000 which was amended in the year 2008. The IT Act amends some provisions of our existing laws i.e. the Indian Penal Code, 1860; the Indian Evidence Act, 1872; the Bankers Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934. Moreover, cyber crime is not a matter of concern for India only but it is a global problem and therefore the world at large has to come forward to curb this menace. Further, complicating cyber crime enforcement is the area of legal jurisdiction. Though the issue of jurisdiction in cyberspace cannot be settled spontaneously, but still a global effort in this direction is the need of hour. The process of crime prevention essentially requires cooperation and active support of citizens, institutions, industries and the government alike.

REFERENCES

[1] International Merchandise Trade Statistics: Compilers Manual, Revision 1 (IMTS 2010-CM), prepared by United Nations Statistics Division, available at http://unstats.un.org/unsd/statcom/doc12/BG-IMTS2010-CM.pdf

[2] The World Information Society Report, 2007, available at: www.itu.int/wisr/

[3] Internet Domain Survey, July 2007, available at: www.isc.org/index.pl?/ops/ds/reports/2007-07/

[4] New Hacker's Vocabulary Dictionary - third edition compiled by Eric S. Raymond, The MIT Press

[5] http://www.thehindubusinessline.com/2000/09/27/stories/242739g4.html

[6] http://www.hackinthebox.org/modules.phpop=modload&name=News&file=article &sid=2683

[7] D Baibridge, Introduction to Computer Law, 4th Ed. 2000

[8] The Audit Commission of the UK since 1987-90 study report, available at https://www.gov.uk/government/publications

[9] http://www.ciol.com/rs-crore-conversion-fraud-busted

[10] M.K. Nagaraja, "Cyberporn Crimes: An Analytical Approach to Investigation", CBI Bulletin, July 2000, p. 25

[11] http://lawmantra.co.in/tamil-nadu-v-suhas-katti-2004-case-related-to-the-posting-of-obscene-messages-on-the-internet/

[12] Avinash Bajaj V/s State (N.C.T.) of Delhi 116 (2005) DLT 427

[13] Shibani A Rao, "Cyber Stalking: A Real Problem in the Virtual World", Lawyers Collective, March 2002, p. 22

[14] Smc Pneumatics (India) Pvt. Ltd vs Shri Jogesh Kwatra on 12 February 2014 http://indiankanoon.org/doc/31110930/

[15] Tata Sons Limited Vs. Respondent: International and Anr. MANU/DE/0220/2011

[16] New Hacker's Vocabulary Dictionary - third edition compiled by Eric S. Raymond, The MIT Press

[17] M. Zakaria Siddiqi, "Cyber Terrorism: Global perspective", The Indian Journal of Criminology and Criminalistics, May-August, 2001, p. 42

[18] http://cybercellmumbai.gov.in/html/case-studies/case-of-fishing.html