# Emerging Trends In Cyber Crime And Challenges Before The Law- (A critical Study)

**Author Rishiraj Singh Nagpal**

*(BBA.LLB 5th Year Law Collage Dhradun Uttranchal University U.K INDIA).*

## 1. INTRODUCTION

The technological development has given rise to a cyber world constituting cyber space. Cyber space is witnessing considerable advancement with the rapid increase in the information technology. It is always hard to determine or predict something in the future in an accurate manner. There is a possibility to consolidate the technological advancements in the past. The internet users are increasing tremendously every year and at the same time there is also rise in the number of people using mobiles and smart phones.

## 2. EMERGING TRENDS & CHALLENGES IN CYBER LAW

Cyber law is likely to experience various emerging trends with the increased usage of digital technology. The various emerging trends include :

a. Challenges In Mobile Laws

b. Legal Issues Of Cyber Security

c. Cloud Computing & Law

d. Social Media & Legal Problems E. Spam Laws

e. Spam Laws

i) *Challenges in Mobile Laws*: Today, there are lots of activities in the mobile ecosystem. The increasing competition has introduced new models of mobile phones, personal digital assistors (pda), tablets and other communication devices in the global market. The intensive use of mobile devices has widened the mobile ecosystem and the content generated is likely to pose new challenges for cyber legal jurisprudence across the world. There are no dedicated laws dealing with the use of these new communication devices and mobile platforms in a number of jurisdictions across the world as the usage of mobile devices for input and output activities is increasing day by day. With the increasing mobile crimes, there is an increasing necessity to meet the legal challenges emerging with the use of mobile devices and ensure mobile protection and privacy.

*ii). Legal Issues Of Cyber Security:* The other emerging cyber law trend is the need for enacting appropriate legal frameworks for preserving, promoting and enhancing cyber security. The cyber security incidents and the attacks on networks are increasing rampantly leading to breaches of cyber security which is likely to have serious impact on the nation. However, the challenge before a lawmaker is not only to develop appropriate legal regimes enabling protection and preservation of cyber security, but also to instill a culture of cyber security amongst the net users. The renewed focus and emphasis is to set forth effective mandatory provisions which would help the protection, preservation and promotion of cyber security in use of computers, allied resources and communication devices.

*iii). Cloud Computing And Law:* With the growth in internet technology, the word is moving towards cloud computing. The cloud computing brings new challenges to the law makers. The distinct challenges may include data security, data privacy, jurisdiction and other legal issues. There pressure on the cyber legislators and stakeholders would be to provide appropriate legal framework that could benefit the industry and enable effective remedies in the event of cloud computing incidents.

*iv). Social Media & Legal Problems:* The social media is beginning to have social and legal impact in the recent times raising significant legal issues and challenges. A latest study indicates the social networking sites responsible for various problems. Since the law enforcement agencies, intelligence agencies target the social media sites; they are the preferred repository of all data. The inappropriate use of social media is giving rise to crimes like cyber harassments, cyber stalking, identity theft etc. The privacy in social media is going to be undermined to a great extent despite the efforts by relevant stake holders. The challenge to the cyber legislators would be to effectively regulate the misuse of social media and provide remedies to the victims of social media crimes. Social Media Litigations are also likely to increase concerning the association or nexus with the output of social media. The litigations regarding defamation, matrimonial actions are popularly increasing and with the data, information resident on social media networking there is an emerging trend of various other litigations in the coming years.

*v) Spam Laws:* There is considerable growth of spam in emails and mobiles. Many countries have already become hot spots for generating spam. As the number of internet and mobile users increase the spammers make use of innovative methods to target the

digital users. It is therefore necessary to have effective legislative provisions to deal with the menace of spam.

## 3. Issues Faced By Cyber Law:

*1) Bazee.Com Case:*

CEO of Bazee.com was arrested in December 2004 because a CD with objectionable material was being sold on website. The CD was also being sold in the markets in Delhi. The Mumbai city police and Delhi police got into action. The CEO was later released on bail. This opened up the question as to what kind of distinction do we draw between internet service provider and Content provider. The burden rests upon the accused that he was the service provider and not the content provider. It also raises also raises a lot of issues regarding how the police should handle the cyber crime cases and a lot of educatioisrequired.

*2.) The Bank NSP Case:*

The bank NSP case is the one where the manager of the bank was engaged to be married. The couple exchanged many emails using the company computer. After some time the two broke up and the girl created fraudulent email ids like “Indian Bar Association” and sent emails to the boy’s foreign clients. She used the bank computer to do this. The boy’s company lost a large number of clients and took the bank to the court. The bank was held liable for using the emails sent using the bank’s computer.

*3.)Parliament Attack Case:*

Bureau of Police Research and Development at Hyderabad had handled some of the topcyber cases, including analyses and retrieving information from the laptop recovered from a terrorist who had attacked Parliament. The laptop which was seized from the two terrorists who were gundown when parliament was siege on December 13 2001, was sent to computer forensic division of BPRD after computer experts at Delhi failed to trace out ofitscontent.

The laptop contained several evidences that confirmed of the motives of the two terrorists, namely the sticker of ministry of Home that they had made on the laptop and posted on their ambassador car to gain entry in parliament house and the fake ID card that one of the terrorist carried with government of Indian seal emblem on it of the emblems (of the three

lions) were carefully scanned and the seal was also craftly made along with residential address of Jammu and Kashmir. But careful detection proved that it was all forged and made on laptop.

*4.)Andhra Pradesh Tax Case:*

Dubious tactics of prominent businessman from Andhra Pradesh was exposed after officials of the department got hold of the computers used by the accused person. The owner of the plastic firm was arrested and Rs. 22 crore cash was recovered from his house by sleuths of the Vigilance Department. They sought an explanation from him regarding the unaccounted cash within 10 days. The accused person submitted 6000 vouchers to prove the legitimacy of the case trade and thought his offence undetected but after careful security of vouchers and content of his computer it revealed that all of them were made after the raids were conducted. It later revealed that the accused was running five businesses of company and used fake and computerized vouchers to use show sales record and save tax.

*5.) Pune Citi Bank Mphasis Call Center Fraud:*

US $ 3,50,000 from account of four US customers were dishonestly transferred to bogus accounts.[1] This will give a lot of ammunition to those lobbying against outsourcing in US. Such cases happen all over the world but when it happens in India it are a serious matter and we cannot ignore it. It is the case of sourcing engineering. Some employees gain the confidence of the customer and obtained their PIN number for commit fraud. They got these under the guise of helping the customers out of difficult situations. Highest security prevails in the call center in India as they know they will lose their business. There was as much as breach of security but of sourcing engineering.

The call center employees are checked when they go in and out so that they cannot copy down numbers and therefore they could not have noted these down. They must have remembered these numbers, gone out immediately to cyber café and accessed the Citi Bank accounts of the customers.

All accounts were opened in Pune and the customers complained that the money from their accounts was transferred to their Pune account and that is how the criminal were traced.

[1]http://www.cyberlawsindia.net

Police has been able to prove the honesty of the call center and has frozen the accounts where the money was transferred.

There is need for strict background check of the call center executives. However best of background checks cannot eliminate the bad elements from coming in and breaching security. We must still ensure such checks when a person is hired. There is need for a national ID and a national data base where the name can be referred to. In this case the preliminary investigations do not reveal that the criminals had any time history. Customers education is very important so customers do not get taken for a ride. Most banks are guilt of doing this. [2]

*6.)State of Tamil Nadu Vs Suhas Katti:*

The case of Suhas Katti is notable for the fact that the conviction was achieved successfully within a relatively quick time of seven months from filing of FIR. Considering that similar cases have been pending in other states for a much longer time the efficient handling of the case that happened to be the first case of cyber crime in the state of Chennai Cyber Cell going to trial deserves a special mention.

The case relating to posting obscene defamatory and annoying message about a divorce woman in yahoo message group. E-mails were also forwarded to the victim for information by the accused to through a false e-mail account opened by him in the name of victim. The posting of the message resulted in the annoying phone call to the lady in the behalf that she was soliciting.

Based on complaint made by the victim in February 2004, the Police traced the accused to Mumbai and arrested him within next few days. The accused was a known family friend of the accused victim and was reportedly interested in marrying her. She however married another person. This marriage later ended in a divorce and the accused started contacting her again. On her reluctance the accused harassed her through internet.

On 23rd day of March 2004 a Charge Sheet was filed u/s 67of IT Act 2000,a69 and 509IPC before the honorable Add. CMM Egnore by citing 18 witnesses and 34 documents and material objects. The same was taken in file in C.C.NO4680/2004. On prosecution side 12 witnesses were examined and entire document were marked as exhibits.

[2] http://www.cyberlawsindia.net

The defense argued that the offensive emails have either given by the ex-husband of the complainant or the complainant himself to implicate the accused as the accused alleged to have turn down the request of the complainant to marry her. Further the defense counsel argued that some of the documentary evidence was not substantial under section 65 B of the Indian Evidence Act. However the court relied upon the court witnesses and other evidence produced before it ,including the witness of the cyber café owners and come to the conclusion that the crime was conclusively proved later Add Chief Metropolitan Magistrate Egmore delivered the judgment on 5-11- as follows-:

"The accused is guilty of the offences under section 469,509 IPC and section 67 of The IT Act 2000 and the accused is convicted and sentenced for the sentenced to undergo Rigorous Imprisonment of 2 years under 469 IPC and to pay fine of rs.500/- and for offence under 67 of IT Act 2000 to undergo 2 years Rigorous Imprisonment for 2 years to pay fine of Rs.4000/-All sentences to run concurrently."

The accused paid fine amount and he was lodged at Central Prison Chennai. This is considered to be the first case convicted under section 67 of the Information Technology Act 2000 in India.

*7.) SMC Pnemanitics India Pvt Ltd. Vs Jogesh Kwarta:*

In India's first case of cyber crime defamation a court of Delhi assumed jurisdiction over the matter where a corporate's reputation was defamed through emails and passed an ex-parte injunction.

In this case the defendant Jogesh Kwarta being an employ of the plaintiff company started sending derogatory, defamatory vulgar, filthy and abusive emails to his employers as also to different subsidiaries of the said company all over the world with the aim to defame the company and the Managing director Mr. R. K. Malhotra. The plaintiff filed a suit for permanent injunction restraining the defendant from doing his illegal acts of sending derogatory emails to the plaintiff.

On behalf of the plaintiff it was contended that the emails sent by the defendant were distinctively obscene, vulgar, abusive humiliating and defamatory in nature.

Counsel further argued that the aim of sending the said emails was to malign the high reputation of the plaintiff's all over India and the world. He further contended that the acts

of the defendant in sending the emails contented had resulted in the invasion of legal rights of plaintiff.

Further the defendant is under a duty not to send the aforesaid emails. It is pertinent to note that after the plaintiff company discovered the said employ could be indulging in the matter on sending abusive emails. The plaintiff terminated the service of the defendant.

After hearing detailed arguments of the counsel of plaintiff the honorable court judge of High Court of Delhi passed an ex-parte 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 obscene vulgar, abusive, derogatory, defamatory, humiliating and abusive emails either to the plaintiffs or its subsidiaries all over the world including Managing Director and their Sales and Marketing departments. Further honorable court restrained the defendant from publishing and transmitting to be published any information in the actual world as also in cyberspace which is derogatory or abusive or defamatory of the plaintiffs.

The order of the Delhi High Court assumed tremendous significant as this is for the first time that the Indian Court assumes jurisdiction in a matter concerning cyber crime defamation and grants an ex-parte injunction restraining the defendant from defamations.

*8.) Sony Sambhandh.Com Case;*

India saw its first cyber crime conviction recently. It all began after complaint was filed by Sony India Pvt Ltd. Which runs a website called argeting non resident Indians. The website enables NRIs to send sony products to their friends and relatives in India after they pay it online.

The company undertakes to deliver the products to the concerned recipients. In may 2002 someone logged onto the website under the identity of Barbara Campa and ordered a Sony Color television set and a cordless head phone.

She gave her credit card number for payment and requested that the products be delivered to Arif Azam in Noida. The payment was duly cleared by the credit card agency and the transaction processed. After following the relevant procedures of due delegence and checking the company delivered the items to Arif Azim. At the time of delivery the company took digital photograph showing the delivery being accepted by Arif Azim. The transaction closed at that but after 45 days that is one and a half month the credit card

agency informed the company that this was an unauthorized transactions the real owner had denied having the purchase. The company lodged an online complaint of cheating Central Bureau of Investigation which registered a case under sections 418,419 and 420 of IPC Indian Penal Code.

The matter was investigated into and Arif Azim was arrested .Investigations revealed that Arif Azim, while working at a call centre in Noida gained access to the credit card number of an American national which he misused on the company's site.

The CBI recovered the colour television and the cordless heard phone. In this , matter ,the CBI had evidence to prove their case and so the accused admitted his guilt. The court convicted Arif Azim under section 418,419 and 420 of the Indian penal code- this being the first time that a cybercrime has been convicted.

The court, however felt that as the accused was a young boy of 24 years and a first time convict, a lenient view needed to be taken .the court there for released the accused on probation for one year . the judgment is of immense significance for the entire nation .beside being the first conviction in a cybercrime matter ,it has shown that the Indian panel code can be effectively applied to certain categories of cybercrimes which are not covered under the information technology act 2000. Secondly ,a judgment of this sort sends out a clear message to all that the law con not be taken for a ride .

*9.)Nasscom Vs. Ajay Sood And Others:*

In the land mark judgement in the case of the National Association and the software companies and the service company v Ajay Sood and others, deliver in March 05. The Delhi High Court declares, (phasing on) the internet to be an illegal act. In telling an injunction and the recovery of the damages elaborating on the concept of the phasing, in order to lay down a precedent in India, the report stated that it is form of the internet fraud where a person pretend to be a illegitimate association, such as a bank and the insurance company in the order to be personal data from a customer such as access codes, password, etc. The personal data collected by the misrepresentation the identity of the illegitimate party is the commonly used for the commonly parties advantage. Court also stated that, by way of an example that the typical phasing scam involve persons who presented online bank and siphon case from the banking accounts after conning customers into handing over confidential banking details. The Delhi High Court stated that even through there is no

specific legislation in India. To analyze phasing, it had phasing to be an illegal act by defining it under Indian law as “a misrepresentation made in the course of trade leading to confusion as to the source and origin of thee mail causing immense harms not only to be consumer but even to the person whose name, identity or password is missed” The court held the act of phasing as passing of tarnishing the plaintiff’s image. The plaintiff in the case was the National association Software and Service Companies (Nasscom) India’s Premier software Association.

The defendant were operating a placement agency involve in head hunting and Service companies recruitment. In order to obtain personal data which they could use for the purposes of the head hunting the defendants composed and sent emails to the third parties in the name of Nasscom. The High Court recoganised the trademark right of the plaintiff and passed an ex-party interim injunction restraining the defendant from using the trade name or anyothers name decepitivly similar to Nasscom. The court further restrain the defendants from holding themselves out as been associate or a part of Nasscom.

The court appointed a commission to conduct a search at the defendants’ premises. Two hard disks of the computers from which the fraudulent emails were sent by the defendants to various parties were taken into custodies by the local commissioner appointed by the court. The offending emails were then downloaded from the hard disks and presented as evidence in court.

During the progress of the case it became clear that the defendants in whose name the defendants emails were sent were fictious identies created by employees on defendants’ instruction to avoid recognition and legal action On discovery of this fraudulent act the fictious names were deleted from the array of parties as defendants in the case. Subsequently the defendant admitted their illegal acts and the parties settled the matter through the recoding of compromise in the suit proceedings. According to the terms of compromise the defendants agreed to pay a sum of Rs.1.6 million to the plaintiff as damages for the violation of the plaintiffs trade mark rights. The court also ordered hard disk seized from defendants, premises to be handed over to the plaintiff who would be the owner of the hard disk.

This case achieves clear milestone it brings to the act of phasing into the ambid of the Indian laws even in the absence of the specific legislation, it clears the misconception that

there is no damage culture in India for violation of IP rights this case reframe IP owner, faith in the Indian judicial system ability and the willingness to protect Intangible Property Rights and send a strong message to IP owners that they can do business in India without sacrificing their IP rights.

## 4. CONCLUSION AND SUGGESTIONS

If you are designing computer software, you actually are designing the core component that would create a Cyber World itself and all aspects of laws in Cyber World would be attracted to it. Therefore, a Technologist working on computers or allied devices or networks needs to be equipped with the fundamentals of the laws surrounding these devices or systems. Ignorance of law is no excuse in the eyes of law. Suggestions to prevent and reduce the incidence of Cyber crimes at domestic level are as follows:

*1. Appointments under the IT Act, 2000:* Fair, Transparent and Speedy Justice Rajesh Tandon, head of the Cyber Regulations Appellate Tribunal (CRAT) is dissatisfied with the „unreasonable" provision relating to the retiring age of the Tribunal"s Presiding Officer and the procedural delay in appointments. Under the IT Act, the presiding officer of a tribunal is required to be either a Judge of a High Court or is/has been a member of the Indian Legal Services and holds/has held a Grade I post in that service for atleast 3 years. The term of a presiding officer has been limited to 5 years from his joining the post or till he attains the age of 65 years, whichever is earlier as per sec. 51 of the IT Act. However, a High Court Judge retires at 62 years and hence he is left with only 3 years term to serve the office. A presiding officer will naturally need time to get adjusted to the new arena of cyber laws. By the time he gets accustomed to the functioning of the tribunal, his tenure is almost over. need time to get adjusted to the new arena of cyber laws. By the time he gets accustomed to the functioning of the tribunal, his tenure is almost over

*2. Information Technology (Amendment) Act, 2008* – Information Technology (Amendment) Act, 2008 is a step in the right direction with the march of time and advance of technology, the problem of Cyber crime is touching alarming dimensions and therefore, calls for concerted action to evolve a universal regulatory mechanism for the prevention

and control of these crimes.[3] In the Indian setting, there is need to inculcate information consciousness among the Indian citizens. Though the Information Technology Act, 2000 as amended in 2008, has reasonably succeeded in providing relief to computer owners/users by extending the reach of law to almost all the online criminal activities and increasing awareness among the people, but it is not a foolproof law as yet since it was primarily enacted for the promotion of e-commerce to meet the needs of globalization and liberalization of economy. The Act still suffers from certain lacunae as it does not provide adequate security against web-transactions nor does it contain adequate provisions to prevent securities fraud, stock confidentiality in the internet trading although the Securities Exchange Board of India (SEBI) has notified that trading of securities on internet is legally recognized and valid.

*3. Need for Modernization of Existing Laws and Enactment of New Laws:* There is a need for modernizing the penal laws of countries which predate the advent of computers. On the one hand, the existing laws have to be changed to cope up with computer-related frauds such as hacking, data theft, software theft, etc. and on the other hand, new legislation is also necessary to ensure data protection and privacy.

*4. Encouragement of Cyber Crime Victims to Lodge Complaints:* In most cases of cyber crime, the victims hesitate to lodge a case. Cyber crime expert Pawan Duggal says that out of every 500 incidents, only 50 get reported, out of these one gets registered. Therefore, the victims of cyber crimes should be encouraged to come forward to lodge complaints against violators of cyber law. Recently, in a first of its kind initiative in the country, Delhi Police has launched a 24x7 helpline for cyber crime victims from January 2008.[4]

*5. Net Security be tightened up :-* Computer technology has proved to be a boon to the commercial world. Perhaps, it is the area which has been most benefited by the advent of computers. Most of the commercial, industrial and business transactions are carried on through internet services at the national as well as the international level. The increasing use of computers in the field of trade and commerce has at the same time opened new vistas for the perpetration of Cyber crimes by the offenders for their personal monetary gain.

[3] Dr. Nuzhat Praveen Khan, "Cyber Crimes and the Adequacy of the Existing Laws", Criminal Law Journal, March, 2006, p-91.

[4] "24x7 Police Helpline to Tackle Cyber Crime", Times of India, December 30, 2010, p-2.

With the liberalisation and globalization of economy, the business houses now believe that there is a huge and profitable market for commercially exploiting the networks. With the increased dependence on computer in commercial field, most of the money transactions are being carried out with the help of comp

uter network making it possible for the cyber criminals to illegally intercept and commit financial frauds. It is therefore, necessary that an adequate security mechanism be developed for safeguarding e-commerce and e-banking against possible online frauds, forgeries, or misappropriation of money etc.[5]

As regards the legality of financial transaction on the internet, the Securities Exchange Board of India (SEBI) vide its notification dated January 25, 2000, has provided that trading of securities on internet will be valid in India but there is no provision to this effect in the Information Technology Act which provides legal validity and prevent security frauds and stock manipulations over the internet. A specific provision for protection of confidentiality in the net-trading, therefore, needs to be incorporated in the I.T. Act.

*6.False e-mail identify registration be treated as an offence:* Cyber criminals often furnish fictitious information while registering themselves for an e-mail address with a website because the email service providers refuse to provide two ID‟s to the same person. This false and misleading information on the internet helps the criminal to suppress his real identity and mislead the investigating authorities in reaching the real culprit.[6] There being no provision in the Information Technology Act to prevent registration of a person for an e-mail address with a website by providing false information, a person can establish false e-mail identity with a fictitious IP address and misuse the same for perpetration of a Cyber crime. This lacunae in the Act has been taken care of by inserting a new Section 66A in the principal Act by the I.T. (Amendment) Act, 2008 (10 of 2009), which provides that any false email identity registration with a website will be an offence punishable upto two years of imprisonment. It is certainly a step forward towards the prevention and control of Cyber crimes.

[5] Dr. S. S. Sharma, “Cyber Crimes and Law in India”, Civil and Military Law Journal, 2004 Jan.- June.; pp-43-52.

[6] Suresh T. Vishwanathan, “The Criminal Aspect in Cyber Laws, 2001, p-81.

## REFERENCES:

*BOOKS:* *1. Informatation Technology Act 2000.*

*2. Cybercrime And Cyber Law In India*

*WEBSITES:*

- *www.indian kanoon.com*
- *www.india .com*