WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Law Relating to Cyber Crime and Judiciary

Rajat Pahuja

Ph. D. Research Scholar, Department of Law, Chaudhary Devi Lal University, Sirsa (Haryana)

ABSTRACT

In every legal system, which accepts the democratic form of government, the Judiciary plays an important role. It is most important wing of the government, which resolves the conflicts among the parties. For the development of the society, the smooth and powerful adjudicative authority is required. The changing nature of the society increases the role of the adjudicatory authority in the present days. In the era of Information and technology, the criminals are using new technology to commit the crime. Therefore, appropriate judicial approach towards the technological offences is required for prevention of the crime. For the proper working of the judiciary the rules of jurisdiction plays an important role. The main problem that is going to face in case of cyber crime is concern with the jurisdiction. India is a developing country. The Indian judiciary is an Independent judiciary. Effective legal machinery can be identified on how properly rules and regulations are drafted by legislation and more importantly how precisely principles of jurisdiction are laid down. A court must have jurisdiction, venue and appropriate service of process in order to hear a case and render an effective judgment. In India, there is only one set of court, which administers national as well as state laws. The constitution has by Article 247, clothed parliament with power to provide for the establishments of additional court for the better administration of law made by the parliament and of any existing law with respect to the matter enumerated in the union list. The courts in India are generally controlled by the state. The courts and the other tribunals are under the superintendents of High court in the territorial jurisdiction of the function. The officers of the courts are appointed by state. The President of India appoints the Judge's of the High Court and Supreme Court. The Indian judiciary is quite independent, because all the laws and conflicts regarding that laws, whether made by center or State going to entertain by the regular court.

Keywords : Independent Judiciary, Legal System, Jurisdiction, Cyber Crime, , Cyber Space

Introduction

The world of Internet today has become a parallel form of life and living. Public are now capable of doing things which were not imaginable few years ago. The Internet is fast becoming a way of life for millions of people and also a way of living because of growing dependence and reliance of the mankind on these machines.through cause of action; it is a combination of computer and crime.In Asia region India has rank top two internet users country, so India is the very fastestgrowing country. Today internet becomes the backbone of social & economic world. Users can access the internet anytime from anywhere but through the internet many illegal works may done. Today E-mail and website is the most efficient way of data communication.The importance to understand the world of crime in the Cyber Space and Technology had been given a priority in India as the crime busted unexpectedly in the Cyber Space and as the criminals became mastermind in the execution of their illegal activities with the use of modern world technologies like computers, smart phones, laptops and other latest digital technologies.

The main object to have a keen observation and study in the area of Cyber Crimes is to stop various kinds of modern crimes like forgery, cheating, blackmailing, theft, robbery, dacoity, etc done with the negative use of technologies and to understand the paten, style or model of the Cyber Criminals with the motive to eradicate or to reduce the Cyber Crime rate in India and for the betterment of the world.

That with the continuous increase of use of e – commerce and e – governance, specifically in this 21th century the computer technologies had even made very easy, fast and possible for the people to communicate with each other by dynamic means to transfer information by sending messages, video calling, text chat etc. Thus being helpful in regulating their business/work in various parts of the world through internet. Such rampant use of various digital technologies had raised a wide variety of legal issues such as piracy, violation of intellectual property, pornography, violation of copy rights, jurisdiction, etc. That in the ground level situations, the proper execution of the concerned laws and the keen probe by an Investigating Personnel plays an important role in delivering speedy and accurate justice to an aggrieved persons/victims but the lack of awareness of the rights and laws made for the citizens of the country can even result in slow down and effect the India's chain of justice delivering system.

The formation of a statutory supervisory body to meet accuracy and transparency in duties and powers of Investigation Agencies can prove to be of good impact for irradiation and reduction of Cyber Crimes or Crimes on whole.

The proper training to the various executive powers and judicial authorities for exercising the cases related to Cyber Crimes and organization of various awareness camps by government can be beneficial and fruitful for the society and its positive growth.

Court's Jurisdiction in Internet Disputes

urisdiction is one of the debatable issues in the case of cyber crime due to the universal nature of the cyber crime. The problem of jurisdiction is not only concern in investigation process but may arise in the trial proceeding also. With the ever-growing arm of the cyber space, the territorial concept seems to vanish. New Methods of dispute resolution should give way to the conventional methods. Thus, the Information Technology Act, 2000 is silent on these issues.

Cyber Crime cannot be territorial but global because internet is network of networks as we have seen earlier. It has wide range of functioning; limiting it to physical boundaries is not possible. Thus even in case of cyber crime their might be a possibility where extra territorial jurisdiction arises. Jurisdiction plays a vital role for undertaking a successful criminal procedure. Dealing with the issue of cyber crime it has been noted that even when investigating officer succeeds in establishing geographical identity of an accused of cyber crime, officer has to face many other difficulties in pursuing his investigation, such as an accused may fall beyond the jurisdictional powers of criminal justice system. In the cyber world where speed is an essence, any attempt to acquire such consent of courts or cooperation will thwart any chance of identifying the culprits and collecting evidence of the crime.

The Doctrine of ubiquity aims determining the place of commission. According to this doctrine, the offence will considered to have been committed in its entirety within a country's jurisdiction, if one of the constituent elements of the offence or the ultimate result occurred within the country's territorial limit. Common Law countries also use effects doctrine in addition to focusing on the physical act. The doctrine locates crime in the territory where it intended to commit or actually took place. Territoriality might grant jurisdiction to many countries in single cyber crime.

Though S.75 provides for extra-territorial operations of this law, but they could be meaningful only when backed with provisions recognizing orders and warrants for Information issued by competent authorities outside their jurisdiction and measure for cooperation's for exchange of material and evidence of computer crimes between law enforcement agencies.

As we are known that internet is network of networks, and thus in the field of cyber space no activity is subject to any one particular jurisdiction. In such cases, territorial borders have no relevancy. For Example: A person who is resident of China, with the use of system of some another country, might commit a crime in India. In such a case what will be the territorial nexus of India? And under what circumstances it can bind such an accused for conviction? To settle this question the Court must have the universal jurisdiction and that must be recognized all over the world.

Universal Jurisdiction Approach

Universal jurisdiction is the new concept, which is emerged, in the international society due to the recent development. The principal of universality is controversial due to various reasons. The main reason for the controversy of this concept is the political and jurisdictional sovereignty of the nations of the world. Though the sovereignty of the state is well emerged, however the globalization and due to special situation for humanity, the municipal laws cannot insure the effective administration of justice. The problem of jurisdictional aspect cannot be excuse for the criminal justice; State has to provide justice on any account in the present welfare state. This problem of jurisdiction does not ensure the justice in certain nature of crimes and criminals particularly in cyber cases. This universal jurisdiction never ensure alternate jurisdiction, it merely provide additional jurisdiction. When the municipal law is unable to provide justice due to the present structure then the universal jurisdiction can apply to provide justice.

Computer Generated Evidence and their Admissibility

Once the jurisdiction is conforming then another important issue is the admissibility of evidence. Therefore, the Indian Evidence Act deals with the Evidence and its admissibility. This act is applicable to all kinds of proceeding, civil and criminal. Generally, in criminal proceeding, the guilt of the accused must proved beyond the reasonable doubt. If any doubt arises, the benefit of doubt always goes to the accused. Therefore, the evidence in criminal proceeding must clear and beyond the reasonable doubt. In traditional crime, the evidence can be collected which may be in the direct form. As like the weapons and the object or the subject matter in the damage form, however this is not possible in the cyber crime. The evidences in cyber crimes are usually unable to collect in the physical form therefore; they cannot produce in the court as like the evidences in traditional crime and trials in traditional crimes. The concept of evidence has to be discussed in two aspect at the time of investigation and during the trial. Therefore, the applicability and admissibility of computer evidence is base on the different footing. Therefore, the Indian Evidence Act has amended to make computer-generated evidences admissible in the court of law. To meet with these challenges, the Amendment made in the existing law, without which the cyber law of India that is Information technology Act cannot work. Section 3 of the Indian evidence act has amended which include the electronic record in the evidence. The insertions of section 65A and Section 65 B in the second schedule are the most important among the amendments, which contended special provision as to evidence related to electronic records.

The sections enacted by considering the nature of the computer crimes and the electronic evidences. The constitution of this section shows the specialty of the evidences in the technical offences as like the cyber crimes. The criminal court follows the general rules of evidence in trial and the conventional evidence is generally appreciated in the court of Law. The cyber crime is quite different due to its mode of commission; therefore, it is not having the evidence as like the conventional crime. The effect of conventional crime can be seen by the common man, as like theft or the grievous hurt can be prove by the statements of the common person, because it can perceived by our senses. However, the effect of cyber crime is though danger than the conventional crime but cannot see by a common person. Therefore, it must be prove on the different bases and it can appreciate on the different principles. If we see

the wording of Section 65A and 65B, it shows some, different from the general evidence which are going to produced in the general court in the conventional trial.

Section 65-B Admissibility of Electronic Records:

1) Notwithstanding anything contained in this Act, any information contended in an electronic record which is printed on a paper, stored, recorded on copied in optical or magnetic media produced by a computer(herein after refer as a computer output)shall be deemed to be also document, if the condition mention in this section is satisfied in relation to the Information and computer in question shall be admissible in any proceeding, without further proof or production of the original or any fact stated there in or which direct evidences would be admissible.

2) The condition referred to in sub-section (1) in respect of a computer output shall be the following, namely:-

a) The computer output containing the information was produced by the computer during the period over which the computer was need regularly to store or process information for the purpose of any activities regularly carried on over that period by the person having lawful control over the use of computer;

b) During the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly feed into the computer in the ordinary course of the said activities;

c) Throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during the part period, was not such as to effect the electronic record or the accuracy of its contents; and

d) The information contended in the electronic record reproduced or is derived from such information feed into the computer in the ordinary course of the said activities.

Where over any period, the function of storing or processing information for the purpose of any activities or any regularly carried on over that period as mention in clause (a) of sub-section (2) was regularly perform by computer whether-

(a) By a combination of computers operating over that period; or

(b) by different computer operating in succession over that period; or

(c) by different combination of computer operating in succession over that period, or

(d) in any other manner involving the successive operation over that period, in whatever order, of any or more computer and one or more combinations of computer. All the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.

(3) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say,—

(e) identifying the electronic record containing the statement and describing the manner in which it was produced;

(f) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;

(g) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(4) For the purposes of this section,—

information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;

(h) whether in the course of activities carried on by any official information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;

(i) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

Explanation: For the purposes of this section, any reference to information being derived from other information shall be a reference to its being derived there from by calculation, comparison or any other process;

Thus, the amendment in the Evidence Act leads to recognize the electronic evidence and its admissibility. The wording of the amended section brings the electronic data and the material under the preview of the Evidence Act. Otherwise, the working of court is impossible because the evidence act originally never recognized the electronic data. Therefore, it is necessary to bring the computer and its generated things under the regular criminal trial. The interpretation of various provisions of IT Act has made according to the natural meaning flowing from it. The recent pronouncement of Supreme Court stating that the recording of evidence through video conferencing is valid in law under section 273 of Criminal Procedure Code has an appreciable development in the field of appreciation of evidences.

Judicial Perspective of India in cyber crime:

The current litigation system of India is not only antique in nature but has become cumbersome and time consuming as well. The backlog of cases is increasing day by day affecting the outcome of various cases. There is an emergent need of judicial and legal reforms in India so that courts in India can meet the expectations of the 21st Century. This can done only by maintaining a stance that preserves the courts reputation and supports the courts critical role in maintaining public confidence in the protection afforded to them by the law. The Indian conventional laws are yet not suitable to deal with the correct issues, the laws regarding to cyber law and Information Technology sector are far away from the real need. The Indian system already facing the problem of low conviction rate in the all criminal matters, and the cyber crime and new technology has created the much hurdles in the said aspect.

Indian Penal Code is universal criminal law of Indian legal system. However, it amended time to time, however its implementation is also not satisfactory in the view of people. The public confidence in the Criminal Justice System of India is declining and the same has forced the Government of India to bring this issue write back to the top of the political agenda. Its aim is to cut crimes by increasing the number of criminals brought to trial and reducing the time taken to complete the legal process. Apart from that, the trial brings before the court, the appropriate appreciations of evidences and the conviction on that matter. Mere proper investigation is not sufficient but the proper appreciations of the evidences by the court is also necessary for the effective criminal justices system.

The Indian Legal system passed the Information Technology Act in 2000, the Act as contended previously is enacted for the regulation of e-commerce. However having certain penal provision but they are not sufficient to curtail the offences takes place by using computer as a tool or target. The various judgments of the Honorable High Courts and the Hon'ble Supreme Court are prima facie based on the provisions of the traditional criminal law, i.e. Indian Penal Code.

Anvar P.V. vs. P.K. Basheer and others

In this significant judgment, the Supreme Court has settled the controversies arising from the various conflicting judgments as well as the practices being followed in the various High Courts and the Trial Courts as to the admissibility of the Electronic Evidences. The Court has interpreted the Section 22A, 45A, 59, 65A & 65B of the Evidence Act and held that secondary data in CD/DVD/Pen Drive are not admissible without a certificate U/s 65 B(4) of Evidence Act. It has been elucidated that electronic evidence without certificate U/s 65B cannot be proved by oral evidence and the opinion of the expert U/s 45A Evidence Act cannot be resorted to make such electronic evidence admissible.

1. The judgment would have serious implications in all the cases where the prosecution relies on the electronic data and particularly in the cases of anticorruption where the reliance being placed on the audio-video recordings, which are being forwarded in the form of CD/DVD to the Court. In all such cases, where the CD/DVD are being forwarded without a certificate U/s 65B Evidence Act, such CD/DVD are not admissible in evidence and further expert opinion as to their genuineness cannot be looked into by the Court as evident from the Supreme Court Judgment. It was further observed that all these safeguards are taken to ensure the source and authenticity, which are the two hallmarks pertaining to electronic records sought to be used as evidence. Electronic records being more susceptible to tampering, alteration, transposition, excision, etc. without such safeguards, the whole trial based on proof of electronic records can lead to travesty of justice. State of Tamil Nadu vs. Suhas Kutti,

It was the first conviction case under the Information technology Act, 2000. Indian court firstly convicted for the offence of cyber crime. The judgment was pronounced in the year 2004, within the seven month after filling the FIR, which brings the conviction for the cyber crime. The Honorable Judge of the Additional Chief Metropolitan Magistrate has passed the order of conviction. In this case, the victim was a divorcee who constantly harassed by annoying phone calls presuming that she would solicit them because of a massage posted on yahoo message group followed by forwarding emails. The massage was extremely obscene, defamatory and annoying. The accuse turn out to be her family friend and interesting in marrying her.

The accused held guilty of offences under Section 469, 509 IPC and 67 of IT Act 2000. The accused had convicted and sentenced for the offence to undergo RI for 2 years. Under section 469 IPC to pay fine of Rs.500/-and, for the offence u/s 509 IPC sentenced to undergo 1 year Simple imprisonment and to pay fine of Rs.500/-, and for the offence u/s 67 of IT Act 2000 to undergo rigorous imprisonment for 2 years and to pay fine of Rs.4000/- All sentences to run concurrently. In the said case the offences registered under Indian Penal Code, though the entire illegal activity were perform by the accuse by using the computer and the internet, The Information technology Act 2000, mere provide punishment for publishing of information which is obscene in electronic form. This provision has not contended about the specific act whether the obscene material is about a particular person or victim. Therefore, the Indian Penal code is requiring for the specific act. Accuse in this case publishing the obscene material regarding a victim, who is the widow of his friend, accuse is having family relation with the victim. Accuse intentionally posting post on yahoo messages grouped followed by the forwarding of emails. The massage was obscene, defamatory and annoying. The Section of the Information technology cover the obscenity but Indian Penal Code

has provided the special provisions regarding forgery for purpose harming reputation under section 469; the I T Act has not provided any provision regarding this specific act or offence. Therefore, the Asst. Commissioner of Police, Cyber Crime Cell, C.C.B. Egmore, Chennai, has filed the Final Report against the accused.

Nirav Navinbhai Shah & 4 ors. Vs. State of Gujarat

The applicants, original accused in crime I.C.R. No. 54 of 2004 dated 26.02.2004 registered with sector 7 police station Gandhinagar for offences punishable under sections 381, 408, 415, 418, 420 read with sections 34 and 120B of the Indian Penal Code and section 66 and 72 of the Information Technology Act, 2000 (herein after referred to as 'the IT Act for short) have preferred this application under section 482 of the Code of Criminal Procedure 1973. (herein after referred to as 'the code' for short) for quashing of FIR I.C.R. No. 54 of 2004 dated 26.02.2004 registered with Sector No. 7 Police Station, Gandhinagar and the resultant Criminal Case No. 54 of 2004 dated 26.02.2004 registered with sector No. 7 Police station Gandhinagar and the resultant Criminal case No.3528 of 2004 pending before the Judicial Magistrate First Class Gandhinagar, mainly on the grounds that the facts and allegation leading to lodging FIR show that the real dispute was a civil dispute and as the same has been amicably settled between the parties, no useful purpose would be served in continuing the criminal proceedings, rather continuation of same would be counterproductive to the interest of justice.

1. The complaint also does not contain any essential ingredient for maintaining criminal proceeding for the alleged offences. As it's stated in the arguments of the learned counsels that the parties have filed civil suits also in respect of the same dispute. The entire dispute between the parties is resolve by amicable settlement. The alleged hacking is perpetrated on the complainants computer system only which said to have data pertaining to its client. The Counsels have submitted that on some of the web sites these data are already available. The dispute appears to be private in nature. The offence alleged is not strictly affecting or infringing any other individual or citizen. Thus looking to the nature of the disputes, it can well be said that continuation of the same is not in interest of justice. It was held that the FIR 54 of 2004 registered at sector 7 Police Station Gandhinagar and resultant Criminal Case No. 3528 of 2004 pending before the JMFC Gandhinagar deserve to be quashed in the interest of just and hereby they are quashed. Rule is made absolute.

The case is deals with Ritu Kohli's case. offence of cyber stalking. Where in the young Indian girl being cyber stalked by a former colleague of her husband, by sending obscene massages ad emails. The Delhi Police arrested Manish Kathuria the culprit of the case. In the said case, Manish was stalking a person called Ritu Kohli on the Net by illegally chatting on the website www.mirc.com with the name of Ritu Kohli. Manish was regularly chatting under the identity of Ritu Kohli on the said Website, using obscene and obnoxious language, was distributing her residence telephone number and inviting chatter to chat with her on telephone. Consequently Ritu Kohli was getting obscene calls from different chatters from various parts of India and abroad. Ritu Kohli reported the matter to the police and the Delhi Police swung into action. The police had registered the case under Section 509 of the Indian Penal Code for outraging the modesty of Ritu Kohli.

The Indian Penal Code, section 509 deals with the words or gesture intended to outrage the modesty of woman, but it does not deals with the massages through the internet or computer. Even the IT Act 2000 also not deals with such kind of crime. None of the Act and the section deals with such kind of act. In such situation after all the Indian penal code, conventional criminal law and the sections can use to deals with such kind of offences. Section 503 of Indian penal code deals with the sending the threading emails, but it not cover the modesty. This case compels the Indian legal system to enact the effective rules, which include the stalking. Due to this Section 66A of the Information Technology Act, 2008 (Amendment 2008) is inserted which states, "Punishment for sending offensive messages through communication service, etc. Indian Penal Code also dealing with the stalking under section 354 D, which is included by the Criminal Law Amendment Act, 2013.

Thus the Cyber crime are going to be adjudicated by the Indian Courts, while dealing with the cyber crime the Court is more depends on the conventional Criminal Law, that is Indian Penal Code. Because the cyber crime is not to much differ than the conventional crime. All the cases, which are known as important cases of cyber crime in India are subjected to the Indian Penal Code. Though the special law that is Information Technology Act 2000 is recognized as cyber law of India, but cyber crime are more concern with the Indian penal Code, without applying the traditional criminal law, the law enforcing agencies cannot work. All the cases discuss here are subject to the Indian Penal Code, and this conventional criminal law provides the relating section to all the offences, which are recognized as a cyber crime. Therefore, the cyber crime and the conventional crime are not different from each other, however the techniques, which are going to use for performing the crime, are different and subjected to the cyber world or cyber space is use to commit the cyber crime.

Conclusion

The computer crime and the crime, which are going to commit by using the computer techniques, can be prevent by the cooperation of the every one form the international community, every State, executive, Judiciary and mainly the alertness of the users of the computer or even a common person. The cyber crime and the conventional crime are quite similar and the implementations never require any special laws, however it needed the change in the procedural aspect of the laws and the forensic techniques for the implementation of the criminal laws for better protection of the people from this crime. Judiciary plays an important role and also wing of the government in resolving the conflicts among the parties in cybercrime. Before going into this research paper, lets know what is cyber- crime. Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal

information, business trade secrets or use the internet for exploitative or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers. In this research paper we will be discussing about how judiciary played role in cyber crime cases. So many amendments were made in other Acts and also there are many landmark judgments to know how judiciary played role in solving disputes related to cyber crime of different type.

REFRENCES

http://www.researchgate.net

www.legalserviceindia.com

Shodhganga.inflibnet.ac.in

Information Technology Act,2000

Cyber Law Cyber crime Internet And E-commerce: By Vimlendu Tayal, Bharat Law Publication, Jaipur, 2011

Cyber Law in India (Law on Internet) By Dr. Farooq Ahmed, New Era Law Publications Delhi, 2005, Pioneer Books.

Cybercrime; Talat Fatima, Eastern Book Company Lucknow.

E-Justices- Practical Guide for the Bench and Bar, By K. Pandurangan, Universal Law Publication, Edition 2009.

Forensic Science in Criminal investigation – Manoobhai G. Amin & Dr. Jai Shankar Singh, Unique Law Publishers, Jodhpur, Edition 2009

Forensic Science in Criminal Investigation and Trials By B.R.Sharma, Universal Law Publication, Fourth Edition, 2003.

Guide to Cyber Law – Rodney D. Ryder