"Authorities Under I.T.Act, 2000: With Special Reference To Cyber Appellate Tribunal In India"

Jamshed Ansari

Asstt. Professor (Guest Faculty), Faculty of Law, University of Delhi, Delhi (INDIA)
E-Mail- jamshedansari024@gmail.com
Date: 14.05.2014

Abstracts: *The author aims to examine the different Authorities under Information Technology Act, 2000 with special reference to Cyber Appellate Tribunal. For this purpose the author had to go through the powers, functions and duties of such authorities with respect to their respective domain. It is better for a city to be governed by a good man than even by good laws. For the better implementation of the mandate of the Information Technology Act, 2000, the proper authorities are required and that the IT Act itself made provision for the same. The author has formulated the following questions and has tried to find out the answer- What are different Authorities under IT Act, 2000? Whether appointment of Chairman of the CAT as per the guidelines given in Judges Appointment case is proper. Whether the provision taking away the power of judicial review is in violation of basic structure of the Constitution of India. Whether the Authorities given in IT Act is sufficient for the better implementation of mandate of IT Act, 2000. What is the role of High Court under IT Act, 2000?*
[Ansari, Jamshed. **Authorities under I.T. Act, 2000: With Special Reference to Cyber Appellate Tribunal in India.** *Academ Arena* 2014;6(6):48-54]. (ISSN 1553-992X). http://www.sciencepub.net/academia. 5

Key Words: *Cyber Appellate Tribunal, cyber crime, regulatory authorities, digital signature, authentication etc.*

Introduction:

"It is better for a city to be governed by a good man than even by good laws" --- Aristotle.

This paper presents the role of different authorities under IT Act, 2000. Internet is an open system of communication, which has its own set of problems. These problems relate to integrity, confidentiality and authentication of communication channel and processes. Since the computerized environment is more process based than personalized, it is hence necessary to have an identification strategy to ascertain the integrity, confidentiality and authentication of communication channels and processes. Any identification strategy required to understand the universality of principle of internet and the World Wide Web linking countries and strangers seamlessly. It is not merely the question of efficiency but also of reliability. The question are- Who shall perform this identity authentication function? Who shall authenticate that a digital signature belongs to a specific signer? Who shall be the dispenser of the public keys?

Authorities Under I.T. Act, 2000:

The Act provides a hierarchy of regulatory authorities having their respective administrative set-ups to try cyber-crime offenders. To solve the abovementioned problems the Information Technology Act, 2000 makes provision for the following regulators or authorities:-

a) Certifying Authorities
b) Controller of Certifying Authorities
c) Adjudication Officer
d) Cyber Appellate Tribunal
e) High Court
f) Criminal Administration is being looked by Magistrate
g) Cyber Police

Each of the above mentioned authorities under the IT Act has its role to play in their respective domain. We would discuss the above authorities one by one.

Certifying Authorities:

In e- transactions the parties are not required to come face to face with one another, for the proper identification of the transactions a third party is required. That is in the form of "Certifying Authority".

A Certifying Authority is a body which may either be public or private that seeks to fill the need for trusted 3rd party services in e- commerce by issuing digital signature certificates. The role played by the Certifying Authority is akin to that of a notary public in the real world. A notary assets that the person who signs the document is really that person. Similarly, a Certifying Authority grants digital signature certificates to subscribers after proper identification and verification.

Certifying Authority is defined under Section 2 (1) (g) as "Certifying Authority" means a person who has been granted a licence to issue a Digital Signature Certificate under section 24. In other words, we can say that a certifying authority is empowered under the IT Act through a licence to grant digital signature certificate as per the provisions of Section 24 of the same Act.

Function and Purpose of Certifying Authority

The purpose of certifying authority may be defined as "a body, either public or private, that seeks to fill the need for trusted third party services in electronic commerce by issuing electronic signature certificate that attest to some face about the subject of the certificate." The certifying authority needs to verify the authenticity of the source of the document.

The certifying authorities are required to perform the following four basic functions to satisfy the needs of their subscribers. These functions are as follows-

1. Processing requests and issuance of digital signature certificate
2. Certificate status information: maintenance of records of current, suspended and revoked digital signature certificate,
3. Directory of current digital signature certificate and certification revocation lists and access procedure by subscribers
4. Achieves of expired digital signature certificates.

Issuance of Certificate by a Certifying Authority:

The "certificate" which is issued by a certifying authority is a computer based record as to the connection between the private key and the corresponding public key. The certificate usually contain the public key along with the other relevant information, like the name of the certifying authority, algorithm of the key, type of key and any licences or the qualifications held by the holder of the key. Subscriber can then disseminate the certificates to the third parties who may wish to communicate with the subscriber. The certifying authority authenticate digital signature by, registering key pairs to individuals. Then, when approached, the certifying authority verifies the integrity of the key pair and links the signature back to the registered owner.

Procedures to be Followed by the Certifying Authority:

As per the provisions of Section 30 of the IT Act, 2000 every Certifying Authority has to follow certain standards to maintain the integrity of its functions. Subsection (a) of Section 30 says that the certifying authority is obligated to use the hardware, software and procedures that are secure from intrusion and misuse. Subsection (b) further, provides that the certifying authority shall provide a reasonable level of reliability in its services which are reasonability suited to the performance of its functions. Subsection (c) provides that a certifying should "adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured." Section 30(ca) states that the certifying authority will be the repository of all electronic signature certificates issued under the Act, and subsection (cb) states that it shall publish its practices, electronic signature certificates and current status of such certificates. Section 30(d) further mandate that certifying Authority shall observe such other standards as may be specified by regulations. IT (Certifying Authority) Regulations, 2001, which was subsequently amended in 2009. Further, Section 31 makes it statutory duty of the Certifying Authority to ensure compliance by its employees and other people engaged to the provisions of the IT Act, 2000 and the rules, regulations and orders made thereunder.

As per the provisions of Section 33(1), on the suspension or revocation of the licence to issue Electronic Signature Certificates issued to a Certifying Authority, the Certifying Authority is mandated to surrender the licences to the controller of the certifying authority.

Controller of Certifying Authority:

A Controller of Certifying Authority is the apex authority in the public key infrastructure. It has not only to formulate rules and guidelines for Certifying Authorities but also as an administrative body has to ensure that these rules and guidelines are followed by the certifying authorities in a proper manner. "Controller of certifying authority" has been defined under section 2(1) (m) of the IT Act, 2000 which says "controller" means the controller of certifying authorities appointed under Section 17(1) of the IT Act, 2000.

Appointment of Controller of Certifying Authority:

Section 17(1) empowers the Central Government to appoint not only a Controller (CCA), but also appoint such number of Deputy Controllers, Assistant Controllers, as it deems fit. The office of Controller has three departments-

(a) Technology Department;
(b) Finance and Legal Department;
(c) Investigation Department,

each having a Deputy Controller and Assistant Controller who works under the general superintendence and control of the Controller of Certifying Authorities. After the 2008 amendment to Information Technology Act, 2000, the Central Government is empowered to appoint such number of officers and employees in addition to Deputy Controllers and Asst. Controllers, by notifying in the Official Gazette.

This section further empowers the Central Government to prescribe the qualifications, experience, terms of service of the Controller, Deputy Controllers, and Asst. Controllers, other officers and employees. Central Government is also empowered to specify the Head Office and Branch Offices if any of the Controller. Currently the Office of the Controller is in New Delhi in the Ministry of

Communication and Information Technology. The office of the Controller is a body corporate having a seal of its own.

In China, the State Council Department in charge of Information Industry (SCDIII) performs functions similar to the Controller under the Information Technology Act, 2000 (India). In Australia it is the Australian Government Information Management Office (AGIMO).

The Role of Controller of Certifying Authorities:

A "controller" has a major role to play with regard to electronic certification services. It has not only to formulate rules and guidelines for Certifying Authorities but also as an administrative body has to ensure that these rules and guidelines are followed by the certifying authorities in a proper manner. The role of Controller of Certifying Authorities (CCAs) is to regulate the functioning of the Certifying Authorities (CAs).

Powers and Functions of Controller of Certifying Authorities:

Section 18 enumerates various powers and functions of the Controller of Certifying Authorities (CCA). The Controller's main function is to regulate and control almost every activity of the Certifying Authorities (CA's). Being the apex authority in the PKI hierarchy, a duty is cast upon the Controller to ensure proper working of the Certifying Authorities and to ensure the safety, security and integrity of electronic signatures. To ensure this the Information Technology Act empowers the Controller of Certifying Authorities to perform certain functions.

The Controller is empowered to supervise the activities of the Certifying Authorities (CA). It is the Controller who issues licences to issue Electronic Signature Certificates to the Certifying Authorities.

Section 18(a) has to read along with Rule 31(2) of the Information Technology (Certifying Authority Rules, 2000 stipulates that the Certifying Authorities shall conduct half yearly audit of the security policy, physical security and planning of its operations and the repository. The Certifying Authority shall submit copy of each audit report to the Controller within four weeks of the completion of such audit and where irregularities are found, the Certifying Authority shall take immediate appropriate action to remove such Irregularities.

The Controller of Certifying Authorities shall certify the public keys ofthe Certifying Authorities. The Root Certifying Authority of India established by the Controller is entrusted to certify/digitally sign public keysof all certifying authorities in India. The Root Certifying Authorityof India (RCAI) is operated as per the standards laid down under the Information Technology Act. The requirements to be satisfied by the RCAI include the following:

(a) The licence issued to the Certifying Authority is digitally signed by the CCA;

(b) All public keys corresponding to the signing private keys of a Certifying Authority are digitally signed by the Controller of Certifying Authorities;

(c) That these keys signed by the Controller of Certifying Authorities can be verified by a relying party through the Controller's website or Certifying Authorities own website.

The RCAI is operated using *Smart-Trust software*. Authorized CCA personnel initiate and perform Root Certifying Authority functions in accordance with the Certification Practice Statement of Root Certifying Authority of India. The term Root Certifying Authority is used to refer to the total certifying authority entity, including the software and its operations. It's 'root certificate' is the highest level of certification in India. A root certificate is a self-signed certificate. All certificates below the root certificate inherit the trustworthiness of the root certificate[145]. Section 18(b) of the Information Technology Act, has to be read along with Rule 20(b) of Information Technology (Certifying Authorities) Rules, 2000. The rule states that, the licenced Certifying Authority shall commence its commercial operation of generation and issuance of digital signature only after it has generated its key pair, namely, private and corresponding public key, and submitted the public key to the Controller. One of the main functions of the Controller is to lay down standards to be maintained by the Certifying Authorities. Information technology architecturemay support open standards and accepted defactostandards. However, Rule 6 of the Information Technology (Certifying Authorities) Rules, 2000prescribed certain standards to be followed for different activities associated with the Certifying Authorities functions. Rule 7 of the Information Technology (Certifying Authorities) Rules, 2000, deals with Digital Signature Certificate Standard.

Cyber Police:

Cyber Police is also called as internet police. This is a generic term for police and secret police departments and other organizations in charge of policing internet in a number of countries. The major purposes of Internet police, depending on the state, are fighting cybercrime, as well as censorship, propaganda and monitoring and manipulating the online public opinion. Cyber Crime Investigation Cell is a wing of Mumbai Police, India, to deal with Cybercrimes, and to enforce provisions of India's Information Technology Law namely, the Information Technology Act, 2000, and various cybercrime related provisions of criminal laws, including the IPC. Cyber Crime Investigation Cell is

a part of Crime Branch, Criminal Investigation Department of the Mumbai Police.

Adjudication Officer:

The adjudicating officer is an authority created to adjudicate any contraventions under Information Technology Act, 2000. The power to adjudicate any contravention vests with an adjudication officer. For the purpose of adjudicating whether any person has committed contravention of Information Technology Act, 2000, its rules, regulations**,** directions, orders, which makes him liable to pay compensation, the Central Government shall appoint an officer called the Adjudicating Officer**. He** must be an officer not below the rank of a Director of Government of India or an equivalent officer. The chief responsibility of an adjudicating officer to adjudicate on cases such as unauthorized access, unauthorized downloading or copying of data, spread of viruses, denial of service attack, disruption of computer or computer network, damage to computer, programmes, data, and compensation for failure to protect data by a body corporate etc. Sub-section (1) should be read along with Rule 4of **the** Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003, which deals with the scope and manner of holding inquiry. The adjudicating Officer will have the power to award compensation as she/he thinks fit. However, the pecuniary jurisdiction of adjudicating officer is limited to claim for injury or damage not exceeding five crores rupees, before, deciding on quantum of compensation or penalty, the adjudicating officer should give the contravening person a reasonable opportunity for making defence in the matter. Thus, an adjudicating officer is duty bound to follow the essential principle of natural justice, i.e., *audi alteram partem* (hear the other side).

Qualification for Adjudication Officer:

The qualifications for adjudicating officers will be prescribed by the government and will include both information technology experience and legal/judicial experience. Rule**3** of Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003 deals with eligibility for adjudicating officer.

Adjudication Officer as Civil Court:

Every adjudicating officer shall have the power of a civil court and it shall be deemed to be a civil court for the purpose of Ss. 345and 346of Cr**.P. C** and Order XXIof **CPC**and all proceedings before it shall be deemed to be judicial proceedings.

Factors to be Taken into Account by the Adjudication Officer:

Information Technology Act, 2000 empowers 'Adjudicating Officer' to adjudicate any contravention under Chapter IX of the Information Technology Act, 2000.Adjudicating officer shall have the power of **a** civil court and all proceedings before it shall be deemed to **be** judicial proceedings. While adjudicating the quantum of compensation, the adjudicating officer is required to consider certain aspects. *Firstly,* the quantum of compensation should be calculated on the basis of amount of gain of unfair advantage derived by the perpetrator as a result of the default. To calculate actual amount of unfairadvantage derived from a contravention is fairly difficult. Hence, wherever quantifiable, the adjudicating officer should consider this factor in fixing the quantum of compensation. *Secondly,* adjudicating officer should consider the amount of loss caused to any person as a result of the default. The pecuniary jurisdiction of the adjudicating officer is Rs. 5, 00, 000, 00. If the claim for compensation exceeds Rs. five crores, then it shall vest with competent court. *Thirdly*, while arriving at quantum of compensation; adjudication officer shall also take into consideration the repetitive nature of the default.

Cyber Appellate Tribunal:

The Information Technology Act, 2000 has established the Cyber Appellate Tribunal having appellate jurisdiction. Being an appellate authority it is entitled to exercise its appellate jurisdiction both on fact as also in law over a decision or order passed by the controller of certifying authority or the adjudicating officer. Its power to examine the correctness, legality or propriety or the decision or order passed by the controller of the certifying authorities or the adjudication officer is absolute.

Establishment of Cyber Appellate Tribunal:

The Central government is empowered to establish one or more appellate tribunals but as far as the provisions of Cyber Regulations Tribunal (Procedure) Rules, 2000 is concerned, there shall be only one tribunal and it shall ordinarily hold its sittings at New Delhi.

The rule is flexible as if at any time, the chairperson of the tribunal is satisfied that circumstances exist which render it necessary to have sittings of the tribunal at any place other than New Delhi, the Chairperson may direct to hold the sittings at any such appropriate place.

The name of the "Cyber Regulations Appellate Tribunal" has been changed as "Cyber Appellate Tribunal"

Composition of CAT:

The Information Technology (Amendment) Act, 2008has changed the composition of the Cyber Appellate Tribunal. Some of the changes are: Prior to the amendment, the Cyber Appellate Tribunal consisted of only one person. He was designated as the presiding officer of the Cyber Appellate Tribunal.

After the amendment, the Cyber Appellate Tribunal will now have a Chairperson and such other members as notified be the Central Government. Now the Cyber Appellate Tribunal ceased to be single member body and became multimember appellate body.

Prior to the amendment, the power to appoint the Presiding Officer was exclusively with the Central Government. But after the amendment, the Information Technology Act mandates that the selection of the Chairperson and members of Cyber Appellate Tribunal shall be made in consultation with the Chief Justice of India.

Here the expression "after consultation with the CJI" must be construed in the same manner as the expression "after consultation with the CJI" under Article 217 of Constitution of India as made in SC Advocate on Record Association v. UOI.

After the IT (Amendment) Act, 2008 this Act proposes that the jurisdiction, powers and authority of the Cyber Appellate Tribunal may be exercised by the benches constituted by the Chairperson of the CAT with one or two members of the tribunal as the Chairperson may deem fit. The benches shall sit at New Delhi or at such other places as the Central Government decides in consultation with the Chairperson.

Bar of Judicial Review:

Section 55 bars judicial review with respect to two matters,

1. Against an order of the Central Government appointing any person as the Chairperson of the Cyber Appellate Tribunal, and
2. Any proceeding before a Cyber Appellate Tribunal on the ground merely of any defect in the constitution of a Cyber Appellate Tribunal.

By making the order constituting the Cyber Appellate Tribunal final and barring the judicial review of any proceedings of the Tribunal on the ground of defect in the constitution of the Tribunal, this section ensures the smooth and uninterrupted functioning of the Tribunal. It must have been the intention of the law makers that the proceedings of the tribunal do not get stalled by frivolous or vexatious litigation by busy bodies.

But as per the ruling of Supreme Court in *Keshvanand Bharti case,* the power of judicial review of the HC and the SC is the basic feature of the Constitution and hence the Parliament cannot take away by the amendment of the Constitution under Article 368. Applying the above dicta on Section 55 which takes away the power of judicial review, we can say that parliament has exceeded its limit, hence this section is unconstitutional.

Qualifications for chairperson and members of CAT:

The Cyber Appellate Tribunal shall consist of Chairperson and members, both judicial and non-judicial members.

Qualification of Chairman and Technical Members:

The Chairperson of Cyber Appellate Tribunal shall be a person who is or has been or qualified to be a judge of the High Court. The non-judicial members are envisaged to be bureaucrats who have held the post of Additional Secretary to Government of India or any equivalent post with Central or State Government for a period of not less than one year or Joint Secretary to Government of India or its equivalent post for a period of not less than seven yearsBesides this, the Information Technology also prescribes technical qualification for non- judicial members. The non- judicial members shall only be appointed by the Central Government from amongst persons having special knowledge and professional experience in Information Technology, telecommunication, industry, management or consumer affairs.

Qualification of Judicial members:

The Judicial members shall be appointed from amongst persons who is or has been a member of the India Legal Services and has held the post of Additional Secretary for not less than one year or Grade I of the Indian Legal Services for not less than five years.

Term of Office of Chairman and Members:

The tenure of Chairman or members of CAT shall be five years from the Date on which he enters his office or until he attains the age of 65 years, whichever happens earlier.

Challenge to the term of Office of the Chairman:

This provision came in for challenge by the sitting Chairperson of CAT, Hon'ble Mr. Justice (Retd.) Rajesh Tandon. He aggrieved by the term of his appointment which was for 3 years considering that he would exceed the age of 65 years if the term was extended, filed a writ petition in Delhi HC impugning the constitutionality of Section 51(1). The ground was that the provision offended the constitutional mandate of equality as contained under Art. 14 of the Constitution of India as it mandated retirement at the age of 65 when other comparable enactments provided for retirement at the age of 67. Court dismissed the petition saying the provision is not ultra vires.

Salary etc. of the Chairperson and Members:

As per the provisions of Section 52, The Chairman and members of the Cyber Appellate Tribunal are paid their salary etc. as per the provisions of the Cyber Appellate Tribunal (Salary,

Allowances and other terms and Conditions of Service of Chairperson and Members) Rules, 2009.

Resignation and Removal:

The chairperson or the members of the Cyber Appellate Tribunal may, by notice in writing under his hand addressed to the Central Government, resign his office. As per the provisions of Section 54(2) Chairperson or member can be removed by an order of the Central Government only on the ground of proved misbehavior or incapacity after inquiry made by a judge of the Supreme Court. Further, Central Government is empowered to frame rules to regulate the procedures for the investigation of misbehavior or incapacity.

Powers of Cyber Appellate Tribunal:

a) Powers of superintendence, direction etc.:

The Chairperson can exercise general superintendence over the affairs of the tribunal. He is also empowered to give to give directions in the conduct of affairs of the tribunal. He also presides over the meetings of the tribunals.

b) Power to constitute benches:

The Chairperson has the power to constitute benches of the tribunal with one or two members. Where the benches of the Tribunal are constituted, the chairperson may by order, distribute the business of that Tribunal amongst the benches and also the matters to be dealt with by each bench. Even in the distribution of business amongst the benches, the Chairperson can exercise discretions.

c) Power to transfer cases:

The Chairperson has power to transfer any case to a larger bench during any stage of hearing of that case, if it appears to him or to a Member of the Tribunal that such case ought to be heard by a larger bench. The aforesaid provision is analogous to Section 52C, which deals with the power of the Chairperson to transfer cases. The Chairperson of the Cyber Appellate Tribunal may transfer any case pending before one bench for disposal to any other bench. Chairperson can transfer a pending case either suo motu (without giving notice to the parties concerned) or on the application of any of the parties. If any party files an application for the transfer of a case pending before a bench to another bench for disposal, the Chairperson shall not affect the transfer of such case without giving notice to the parties and hearing them. However, a Chairperson can also suo motu transfer a case to another bench.

d) Power of Tribunal as Civil Court:

The courts in India have generally given a wide meaning to the term while interpreting it in the context of Articles 227 and 136 of the Constitution. The Supreme Court of India has included within the meaning of the term 'tribunal' all those bodies which are vested with the judicial power of the State. According to this section, the Cyber Appellate Tribunal is not bound by the procedure laid down by the Code of Civil Procedure, 1908. Instead the Tribunal shall be guided by the principles of natural justice. Though 'tribunals' and 'courts' have several distinguishing features, both are required to follow certain formal procedures. Both perform judicial function. Tribunals, like courts, have to hear both the parties, have to give findings of facts, rulings on law and decide according to the law. The Cyber Appellate Tribunal shall also have powers to regulate its own procedure including the place at which it shall have its sittings.

e) Cyber Appellate Tribunal shall be deemed to be civil court:

For the purpose of discharging its functions under IT Act, theCyber Appellate Tribunal shall have the powers as are vested in a civil court. Every proceedings before the Tribunal shall be deemed to be judicial proceeding and the Cyber Appellate Tribunal shall be deemed a civil court.

Appeal to Cyber Appellate Tribunal:

Appeal is a formal request to a court or to somebody in authority for a judgment or a decision to be changed. Section **57** of the IT Act contains substantive grounds, as well as procedure for filing an appeal before the CAT. Section **57(1)** grants right to appeal to any aggrieved party, who has been aggrieved by an order made by Controller of Certifying Authority or an adjudicating officer under the ITAct. Sub-section **(1)** of Section **57** has enlarged the scope of right to appeal by including even those persons who were not the 'original' contesting parties before the CCA or Adjudicating Officer in a given case.

This section bars appeal against an order before the CAT if such order was made by the adjudicating officer with the consent of the parties.

Appeal to High Court:

Information Technology Act, 2000 provides for a hierarchy of forums to adjudicate contraventions under the Act. An appeal against the decision of an adjudicating officer or Controller of Certifying Authority shall lie before the Cyber Appellate Tribunal. The Information Technology Actprovides for a second appellate forum to entertain appeal against the order of the Cyber Appellate Tribunal. According to Section 62 of the Information Technology Act, a person aggrieved by the decision or order of the Cyber Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Tribunal. The Cyber Appellate Tribunal is an appellate body against the decision of the adjudicating officer or Controller of Certifying Authority. It constitutes first appeal. Appeal against

the decision of the Cyber Appellate Tribunal before the High Court is second appeal.

Conclusion

For the smooth functioning of any law, such law must be just, fair and reasonable and at the same time there must be a proper forum to regulate it. To give effect to the IT Law, the parliament has established the most important authorities under the same Act for smooth functioning. Internet is an open system of communication, which has its own set of problems. These problems relate to integrity, confidentiality and authentication of communication channel and processes. Since the computerized environment is more process based than personalized, it is hence necessary to have an identification strategy to ascertain the integrity, confidentiality and authentication of communication channels and processes. Internet is an open system of communication, which has its own set of problems. These problems relate to integrity, confidentiality and authentication of communication channel and processes. Since the computerized environment is more process based than personalized, it is hence necessary to have an identification strategy to ascertain the integrity, confidentiality and authentication of communication channels and processes.

References

1. Information Technology Act, 2000
2. The Cyber Regulations Tribunal (Procedure) Rules, 2000
3. Information Technology (Amendment) Act, 2008
4. Consumer Protection Act, 1986
5. Administrative Tribunals Act, 1985
6. Oxford Advanced Learner's Dictionary, 2007
7. Gupta, Apar, Commentary on Information Technology Act, 2000, LexisNexis ButterworthsWadhwa Nagpur Publication, Ed. 2, 2011.
8. Henery Chan, Raymond Lee, Thoram Dillon, Elizabeth Chang, E-Commerce; Fundamentals and Applications, Wiely India Pvt. Ltd.(India), Reprint 2008.
9. Pankaj S., E- Commerce, KulBhusanNangia APH Publishing Corporation, 2005.
10. Sharma, Vakul, Information Technology and Practice, Universal Law Publication, 2008.
11. RohasNagpj*Cyber Crime and Corporate liability (2008),* CCH Walter Kluwers (India) Ltd,
12. Indira Carr, *India joins the cyber-race: Information Technology Act 2000,* Int. TJs* 2000, 6(4), 122-130, (2000)
13. Vakul Sharma, Information technology: Law and Practice, Universal Law Publication, Ed. 2, 2008
14. VivekSood, Cyber Law Simlpified, Fourth Ed., 2008, Tata McGraw-Hill Publishing Company Ltd.
15. ACC v. PN Sharma, AIR 1965 SC 1595
16. www.lawkhoj.com
17. www.legallyindia.com

6/13/2014