Legal Framework for E-Governance: A Critical Analysis of Information Technology Act, 2000

Dr. Inderjit Kumar*

Abstract

Law is an important instrument to control the activities of the human beings. Therefore an approach of law is very crucial and relevant in the field of e-Governance. The subject matter of this research paper is the laws governing of e-Governance. Law is implemented through government agenesis. The legal framework is a system of a country by which state controls the activities of concerned subjects. The legal issue plays an important role in determining the growth and advancement of the infrastructure and its resultant impacts on e-Governance. This rule will apply to all countries and India is not an exception to this rule. Legal issues form a base for governance infrastructure as they constitute inherent management and control tools for the e-Governance initiative. Law on Information Technology and related amendments in this law are the outcome of the United Nations Commission on International Trade Law of 1997.

Key words:- e-Governance, Information Technology Act, 2000, Electronic Records, Electronic Signature, National e-Governance Plan (NeGP).

E-Governance

E-Governance is no more or less than governance in an electronic environment. It is both governance of that environment and governance with that environment, using "Electronic tools." This is a very broad definition reflecting the far-reaching implications of information and communication technologies.[1] In other words e-Governance is not just about government websites and e-mails. It is not just about digital access to government information or electronic payments. It is also not just about service delivery over the Internet. It will change how the citizens relate to governments and how the citizens relate to each other. It will bring forth new concepts of citizenship both in terms of need and responsibilities. E-Governance is a much more massive transformation than electronic service delivery. E-Governance is multi-faceted. It deals with information technology as a tool of governance, an object of government's attention and a major factor in shaping the social and economic environment in which

* Assistant Professor of Law, St. Soldier Law College, Jalandhar, Punjab, e-mail: advocate_inderjit@yahoo.com

[1]Pankaj Sharma, "e-Governance- The New Age Governance" (New Delhi: APH Publishing Corporation, 2012) p 19.

government acts. Looked at this way, e-Governance can and does implicate all aspects of public services.

The Information Technology Act, 2000

Almost all Information Technology savvy have welcomed the *Information Technology Act, 2000* passed by the Indian Parliament on May16, 2000, got Presidential assent. The enactment of Information Technology Act, 2000 is an important step in promoting the use of Information Technology in Government and Business.

The *Information Technology Act, 2000* is a forward-looking piece of legislation. It provides legal recognition to e-Governance. It has become first uniform IT law in India because there was no IT law in the country before IT Act, 2000. The Information Technology law also amends the *Indian Penal Code, Indian Evidence, the Bankers Book Evidence Act* and *Reserve Bank of India Act* to carry out the provisions of this legislation. In India, e-Governance is recognised by *Information Technology Act, 2000*. This act provides legal framework for electronic commerce conducting through computer and transmitted over the computer network through the internet. It also deals with cyber offences such as hacking, publishing, misuse of digital signature certificates and causing damage to the computer system by introducing viruses.

After the Amendment of 2008, to say that *Information Technology Act, 2000* is to facilitate e-commerce only, will be a misnomer. This Act is also meant to promote and facilitate electronic filing of documents with the Government agencies and provide efficient delivery of services to the public by means of reliable e-Governance. To achieve this object central government framed *Information Technology Act in 2000*. It was suffering from lacuna. To remove such lacuna Indian Legislature drafted a bill and same was passed. It was named as "*Information Technology Amendment Act, 2008*". With this Parliament has inserted following new provisions in this Act.

i. New Section to address technology neutrality from its present "technology specific" form (i.e. Digital Signature to Electronic Signature) Section 3A;
ii. New Section to address promotion of e-Governance & other IT application (a) Delivery of Service; (b) Outsourcing - Public Private Partnership Section 6A; this section is the basis of present e-governance system. It promotes public Private Partnerships in e-Governance projects. Central Government and State Government are able to tie up with private companies for the

implementation of e-Governance throughout the country. Common Service Centres (CSCs) are best and successful example of this section.

iii. New Section to address electronic contract Section 10A;
iv. New Section to address data protection and privacy Section 43;
v. Body corporate to implement best security practices Sections 43A & 72A;
vi. Multimember Appellate Tribunal under Sections 49-52.
vii. New Section to address new forms of computer misuse under Section 66A and Pornography under Section 67A.
viii. Preservation and Retention of Data/Information Section 67C.
ix. Revision of existing Section 69 to empower Central Government to designate agencies and issue direction for interception and safeguards for monitoring and decryption Section 69 x. Blocking of Information for public access Section 69A.
x. Monitoring of Traffic Data and Information for Cyber Security Section 69B.
xi. New section for designating agency for protection of Critical Information Infrastructure Section 70A.
xii. New Section for power to CERT-In to call and analyse information relating to breach in cyber space and cyber security Section 70B.
xiii. Revision of existing Section 79 for prescribing liabilities Section 79 of service providers in certain cases and to Empower Central Government to prescribe guidelines to be observed by the service providers for providing services. It also regulate cyber cafe under Section 79.
xiv. New Section for Examiner of Digital Evidence Section 79A.
xv. New Section for power to prescribe modes of Encryption Section 84A.
xvi. Punishment for most of offences was reduced from three years to two years.[2]

There are a number of positive developments, but some of them dismay as well. Positively, they signal the attempt made by the government to create a dynamic policy that is technology neutral. There have also been attempts to deal proactively with the many new challenges that the Internet creates.

It is pertinent to mention here that IT was not made to regulate e-commerce and IT relating offences only. It is important to note that Chapter -3 of the *Information Technology Act, 2000* sections 4-10A deals with e-Governance. The important provisions of the act are following.

i. Legal Recognition of Electronic Records (Section- 4)

[2]Inserted by Information Technology (Amendment) Act, 2008.

ii. Legal Recognition of Digital Signatures (Section- 5)
iii. Use of electronic records and digital signatures in Government and its agencies (Section-6)
iv. Delivery of services by service provider (Section-6A):- (a) Authorisation by the appropriate government to set up, maintain and upgrade the computerised facilities., (b) Service Provider, (c) Collection etc. of Services charges, (d) Government to specify scale of service charges
v. Retention of electronic records (Section 7)
vi. Audit of Documents etc., maintained in electronic form (Section- 7A)
vii. Publication of rule, regulation, etc., in Electronic Gazette (Section-8)
viii. Sections 6, 7 and 8 not to confer right to insist document should be accepted in electronic form (Section-9)
ix. Power to make rules by Central Government in respect of digital signature (Section-10)
x. Validity of contracts formed through electronic means (Section- 10A) [3]

Section- 4 Legal Recognition of Electronic Records:- According to Section 4, the law requires that, any information or matter must be in writing or in hand written form then such requirement shall be deemed to be satisfied if such information is in electronic form. Therefore, Section 4 confers validity on electronic record.

It is obligatory to take Section 4 of the Act into consideration along with amendments /substitutions in *Indian Penal Code, 1860* (Ss. 29A, 167, 172, 173, 174, 192, 204, 463, 464, 466, 470, 471, 474, 476, 477A) and *Indian Evidence Act, 1872* (Ss. 3, 17, 22A, 35, 39, 59, 65A, 65B, 81A, 81B, 90A, 131) introduced by the *Information Technology Act, 2000*.[4]

Publishing of draft regulation by putting the same in the website and issuing public notice in two newspapers and the copies of draft regulations may be obtained from the commission's offices. It would be publication of draft regulation within the meaning of section 23 of the Central General Act, 1894. If a notification is published in the Electronic, the notification is deemed to be published in the Official Gazette and the notification is deemed to be published in the Official Gazette. Where the notification is published both in the Official Gazette and Electronic Gazette, the date of publication shall be deemed to be the date of Gazette which was first published in any form.[5]

In recent case Hon'ble Karnataka High Court held that, "if an acknowledgment is sent by "originator" to the addressee" by e-mail, without any intermediary, it amounts to electronic

[3]The Information Technology Act, 2000.
[4]Vakul Shrama. "Information technology Law and Practice" (New Delhi: Universal Law Publishing Co. 2011) p 49.
[5]Orissa Consumers Association and Anr. Vs. Orisa Electricity Regulation Commission and Ors. AIR 2005 Ori.11

communication. This mode of transaction is legally recognized under Section 4 of the Information technology Act, 2000. New communication systems and digital technology have made dramatic changes in our life style. A revolution is emerging in the way people transact business. Businesses and consumers are increasingly using computers to create, transmit and store information in the electronic form instead of traditional paper documents. Information stored in electronic form has many advantages."[6]

It is cleared by the High Court in above referred judgement, that Section 4 of the *Information Technology Act, 2000* provides that if information or any other matter is to be in writing or in the typewritten or printed form, then, not withstanding anything contained in such law, the requirement is deemed to have been satisfied if such information or matter is rendered or made available in an electronic form and same is accessible to be used for a subsequent reference.

Section- 5 Legal Recognition of [Electronic Signatures][7]:- Section 5 of *Information Technology Act, 2000,* confers validity to the digital signature. It provides that whenever law requires any information or matter must be authenticated by affixing the signature or any mark on any document must be signed by a person, then such requirement shall be deemed to fulfil if such information, matter or document is digitally signed. "Signed", to a person, means affixing of his and written signature or any mark on any document and expression "signature" shall be construed accordingly.

Section- 6 Use of electronic records and [electronic signatures][8] in Government and its agencies:- This section confers validity on use of electronic record and electronic signature in government office and agencies. This section is promoting the government agencies to use electronic means for the facility of general public. It provides, that whenever any form, application or document is to be submitted by a person in a government office then it can be submitted in electronic form. Similarly, when any licence, passport, registration of vehicle, approval or sanctioned is to be issued or granted by authority or officer then it can be done in electronic form. We can receive and pay money to government offices or agencies in electronic form also.

This section is meant for all governmental practices and functions. That aim of this section is to implement e-Governance at gross-root level. Therefore government has also taken important step toward.

[6]Sudarhan Cargo (P) Ltd. Vs. Techvac Engg. (P) Ltd., (2014) 1 ICC 906(Kant.).
[7]Subs. by IT (Amendment) Act 2008, sec. 2, for "digital signature" and "digital signatures"(w.e.f. 27-10-2009).
[8]Subs. by Act 2009, sec. 2, for "digital signature" and "digital signatures" (w.e.f. 27-10-2009).

Section-6A Delivery of services by service provider:- Service Provider (Explanation to Section 6A): This section has become the backbone of e-governance. This provision has inserted in IT act with *IT Amendment Act, 2008*. It empowers the government to implement e-governance. It is important to note that service provider so authorised includes any individual, private agency private company, partnership firm, sole proprietor firm or any such other body or agency which has been granted permission by the appropriate Government to offer services through electronic means in accordance with the policy governing such service sector.

Authorisation by the appropriate Government to set up, maintain and upgrade the computerised facilities [6A(1)]: This section is base of e-Governance in India. It promotes private participation in delivery of e-Government services. This section gives direction to Government to set e-Governance infrastructure services delivery and maintain it properly. It gives a legal recognition to Public Private Partnership (PPP) programme to provide efficient delivery of services using electronic means and further, such service providers to set up, maintain and upgrade the computerized facilities in e-Government domain.

For the purposes of e-Governance and for efficient delivery of services to the public by way of electronic means the appropriate Government may, by notification in Official Gazette, authorise, by order any service provider to set up, maintain and upgrade the computerised facilities and perform such other functions as it may specify.

According to this section, the appropriate government may order any services to the setup, maintain and upgrade the computerized facilities and to provide such services in electronic form. Other features of this section as under:-

Collection etc. of service charges/Service Fees. [6A(2)(3)]: The appropriate Government may also authorise any service provider authorised to collect, retain appropriate such service charges, as may be prescribed by the appropriate Government for the purpose of providing such services, from the person availing such service.

The appropriate Government may authorise the services providers to collect, retain and appropriate service charges under this Section even if there is no express provision under the Act, rule, regulation or notification under which the service is provided to collect, retain and appropriate e-service charges by the service providers.

Government power to specify scale of service charges [6A(4)]: The appropriate Government shall, however, by notification in the Official Gazette, specify the scale of service charges which may be charged and collected by the service providers under this section. [6A(4)]

National e-Governance Plan (NeGP): NeGP seeks to lay the foundation and provides impetus for long-term growth of e-Governance in India. It seeks to create the right governance and institution mechanisms and set up the core infrastructure polices and set up 44 Mission Mode Projects (MMPs) at Centre, State and integrated services levels to create citizen centric and business centric environment for governance.

NeGP Vision: "Make all Government service accessible to common to man in his locality, through common service delivery outlet and ensure efficiency transparency and reliability of such services at affordable costs to realize the basic need of the common man."[9]

E-Governance initiatives are going to change the way people are being served by the government. The World Bank's grant of 2200 crore rupees, through the National e-Governance Action Plan for implementing various projects in mission mode for future, has provided great impetus to these initiatives.[10]

Section-7. Retention of electronic records.- Section 7 deals with retention of electronic records. It provides that when law requires any information, document, or record to be retained for a specified then such documents, information or record must be retained in electronic form. In fact, most of the government offices and departments have started retaining their documents, information and records in electronic form, thus resulting in paperless environment. Therefore, such government offices and departments are free from the hassles of retaining their record in the forms of files for years.

Section-7A. Audit of Documents etc., maintained in electronic form:- This section is again one more step towards creating the importance of electronic documents and auditing of it in electronic form. It articulates that electronic records must also be audited. With increasing digitization, more and more records are being kept in electronic databases; hence the need of hour is to audit such electronic records or electronic database. That the audit period will be according to laws for the time being in forced for that specific area/subject matter. Thus it would be prudent that every department, organization, individual or company has to formulate a detailed plan for retention and purging of electronic records.

[9]Ministry of Electronic & Information Technology, Government of India, "National e-Governance Plan" retrieved from <http://meity.gov.in/divisions/national-e-governance-plan> access on 20-10-2016.
[10]Vakul Shrama, "Information technology Law and Practice" (New Delhi: Universal Law Publishing Co. 2011) p. 53.

Section-8. Publication of rule, regulation, etc., in Electronic Gazette:- This section confers validity on e-gazette. Therefore today, apart from publishing rules, regulations and laws in official gazette, the appropriate government may also publish them in e-gazette.

The legislators have equated the Electronic Gazette at par with the Official Gazette. The proviso further provides that the date of publication shall be deemed to be the date of the Gazette published for first time in any form.

Section-9. Sections 6, 7 and 8 not to confer right to insist document should be accepted in electronic form:- The aforesaid section grants limited e-governance right as it does not confer upon any person to insist that any Ministry or Department of Central Government or the State Government or any authority or body has to accept, issue, create, retain and preserve any document in the form of electronic records or to participate in any monetary transaction in electronic form.

It is pertinent to mention here that section 9 is the biggest barrier on the way of e-governance. On one hand the main aim and objective of the Information Technology Act, 2000 is to facilitate e-Governance however, on the other hand, Section provides that no one can insist any government office to interact in electronic form.

Section-10. Power to make rules by Central Government in respect of [digital signature]:- Section 10 of Information Technology Act, 2000 is conferring powers to Central Government to make rules in respect of Digital Signatures/Electronic Signatures. The amendments have introduced the concept of electronic signatures, which is a much wider concept and includes digital signatures as well.

The section 10 has to be understood by considering following rules as made under the Information Technology (Certifying Authorities) Rules, 2000:- *Rule 3 The manner in which information is authenticated by means of Digital Signature, Rule 4 Creation of Digital Signature, Rule 5 Verification of Digital Signature, Rule 6 Standards, Rule 7 Digital Signature Certificate Standards, Rule 8 Licensing of Certifying, Rule 23 Digital Signature Certificate, Rule 24 Generation of Digital Signature Certificate, Rule 25 Issue of Digital Signature Certificate, Rule 26 Certificate Lifetime*

It is important to note that care should be taken while reading these rules, as the aforesaid rules are vis-à-vis digital signature regime. Thought section 10 has been amended but the corresponding amendment in the Information Technology Rules, 2000 has not yet been made.

Section 10A. Validity of contracts formed through electronic means:- This Section is based on the United Nation's Convention in 1996 on the use of Electronic Communications in International Contracts. The aim and object of Section is to provide legal validity to online contracts. It provides legal

certainty as to the conclusion of contracts by electronic means. It deals not only with issue of contract formation but also with the form in which an offer and acceptance may be expressed.

Legal validity of online contracts provides legal credence to online e-commerce activities, including buying and selling of goods and services. It also covers e-Governance services and contract which a user may enter with e-Governance service provider and it will be legally binded.

Section 79 A. Central Government to notify Examiner of Electronic Evidence:- This is very important section of Information Technology Act, 2000. This is section empowering the Central Government to appoint or authorise any department or any agency for the purpose of Electronic Evidence Examiner.

Section 45A of Indian evidence Act deal with the opinion of examiner of electronic and clarifies that if court forms an opinion on any matter regarding the electronic records in that case court may takes opinion of examiner of electronic. It is pertinent to note this thing that examiner must be authorised by central Government in this regard.

Section 79A of Information Technology Act empower the Central Government to appoint authority for the purposes of providing expert opinion on electronic form evidence before any court or other authority specify by notification in the official Gazette, any department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence.

Relevancy of Information Technology Act, 2000

Information Technology has own importance in the society and legal system. IT Act is also very important in field of e-Governance and we have already discussed the main provisions of it. IT regulates the affairs of government to government, government to business and government to people. Therefore there are some other characteristics of this which are given below;-

(a) Electronic Signature:- Electronic signature is defined under section 2(ta) of Information Technology Act, 2000. Section 3A which deal with electronic signature was inserted in Act in 2008, with the passing of this Act, any subscriber may authenticate electronic record by affixing his electronic signature. “Signed” to a person means affixing of his written signature or any mark on any document and expression “signature” shall be construed accordingly.

(b) Electronic Signature Promote Governance:- Where any law provides submission of information in writing, online or in the typing form, from now onwards there will be sufficient compliance of law, if the same is sent in an electronic form. Further, if any statute provides any affixation of signature in any

document, the same can be done by means of electronic/digital signature. It has also got legal recognition by law under Indian Law of Evidence.

(c) Secured Electronic Records and Digital Signature:- Sections 14 to 16 deal with provision related to secure electronic records and secure electronic signatures. Information Technology, Act empowers the Union Government to prescribe the security procedure in relation to electronic records and digital signature, considering the nature of the transaction, the level of sophistication of people with the reference to their technological capacity, the volume of transaction and the procedure in general used for similar type of transitions/ communication.

(d) Appointment of Controller of Certifying:- The Central Government may appoint a Controller of Certified Authority under section 17 who shall exercise supervision over activities of certifying authorities. Certifying authority means a person who has been granted a licence to issue an electronic/digital signature certificate.

(e) Procedure and Powers of Appellate Tribunal:- Section 57 of IT Act empowers the Tribunal to regulate its own procedure including the place at which it shall have its sittings. Therefore tribunal is not bound by the procedure laid down by the *Code of Civil Procedure, 1908*. Tribunal has the same powers as are vested in a civil court the C.P.C.

(f) Duties of Subscribers:- Information Technology Act prescribes the duties of subscribers under sections 40 to 42. A subscriber can publish or authorise the publication of electronic/digital signature certificate. Similarly, subscriber can accept such certificate. It is the responsibility of a subscriber to exercise reasonable care to retain control of the private key corresponding to the public key listed in his digital signature certificate.

(g) Cyber Appellate Tribunal:- Union Government has the power to establish the Cyber Appellate Tribunal under section 48 of the IT Act, 2000. Cyber Appellate Tribunal has the power to entertain the appeal of any person aggrieved by the order made by the Controller or the adjudicating officer under section 57 of this Act.

(h) Adjudication Provisions and Punishment:- The emerging communication technology inevitably has an immense impact on life of the people in modern time, but the advantages and benefits of global connectivity have brought certain dangers emanating from inter-connectivity of information network with them which provide scope for cyber criminals on their criminal activities in cyberspace. IT Act, sections 65 to 78 provide punishment for offence under the chapter XI. [11]

[11]Dr. Vishwanathan Paraanjape, "Cyber Crimes& Law" *(*Allahabad: Central Law Agency, 2010) p 16.

If any person is found tampering with computer source or document, he shall be punishable with imprisonment upto three years or fine upto 2 lakhs rs. or with both. Similarly, if any person is found hacking a computer system, he shall be punished with imprisonment upto 3 years or with fine which may extend upto 2 lakhs or with both.

If any person is publishing information which is obscene in electronic form, he shall be punished with imprisonment which may extend to five years or with fine upto 2 lakhs. The act has extra-territorial jurisdiction to punish all criminals who commit offence outside India also.

If anyone without the permission of the owner, excesses the owner's computer, computer system or computer networks or download copies or introduce any computer virus or damages computer, computer system or computer network data etc, he shall be liable to pay damage by way of compensation not exceeding rs. 1 crore to the person so affected.

Grey Area of Information Technology Act

After having discussed the important provisions of the Act, attention should also be drawn to some of its loopholes. Act has some weak points. Information Technology is a dynamic concept. It is changing day by day. Therefore, new problems are arising with passage of time. The most serious concern about the Indian Information Technology law relates to its implementation. The IT Act, 2000 does not lay down parameters for its implementation. Also, when internet penetration in India is extremely low and government and police officials, in general, are not very computer savvy, the new Indian cyber law raises more questions than answers. IT is likely to cause a conflict of jurisdiction. It does not provide clear provision regarding the jurisdiction of offences. It does not touch the serious issues relating to domain names. But electronic commerce is based on the system of domain names. Even domain names have not been defined and the rights and liabilities of domain name owners do not find any mention in the law. As the cyber law is growing, so are the new forms and manifestations of cyber crimes. The offences defined in the IT Act, 2000 are by no means exhaustive. However, the relevant provisions of the IT Act, 2000 make it appear as if the offences detailed therein are the only cyber offences possible and existing. The IT Act, 2000 does not cover various kind of cyber crime and Internet related crimes.[12] There are some other issues which are necessary to discuss in detail and are as below:-

[12]R. M. Kamble, "Cyber Law and Information Technology" (International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013) p 789.

(a) Improper Authentication of Digital Signatures:- The act deals only with Public Key Infrastructure (PKI) framework for authentication. It does not recognize any other authentication procedure though the ambit of 'legal record' is wide. This may cause problems for m-commerce transactions that may not necessarily use the PKI system for authentication and security purposes.

(b) Qualifications and Powers of Adjudicating Officers Unclear:- The Act is unclear as to the qualifications of an adjudicating officer and the manner in which he shall adjudicate. Moreover, the statute is supposedly a 'long arm statute', it does not indicate the powers of the adjudicating officers when a person commits a cyber crime or violates any provisions of the law from outside India. Several practical difficulties may also arise while importing the cyber criminal to India. The Act does not lay down any provisions whereby extradition treaties can be formed with countries where the cyber criminal is located.

Therefore, the extra-territorial scope of the Act may be difficult to achieve. Furthermore, the powers to impose a penalty for a computer crime upto Rs. 1 crore offers a large discretion to adjudicating officers and may turn out to be harmful.

(c) Misuse of Police Powers:- The search and arrest powers given to police officers without any definite guidelines may be ill-used and Section 66A is the example of it. Supreme Court of India has declared it void. This section has been widely misused by police in various states to arrest innocent persons for posting critical comments about social and political issues.[13]

(d) Internet Service Provider Liability and Responsibility for Content Regulation not attributable:- While Section 78 absolves a network service provider of its liability if it can prove its ignorance and due diligence, it fails to specify as to who would be held liable for such contravention in such an event. This provision will certainly cause problems when an offence regarding third party information or provision of data is committed.[14]

(e) Intellectual Property Rights Violation:- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011is protected personal and sensitive data. The IT Rules protect information pertaining only to: a) Medical records, b) Physiological, physical and mental health condition, c) Passwords, d) Financial information, e) Sexual orientation, and f) Biometric details.

[13]Shreya Singhal V. Union of India, (2015) 5 SCC 1.
[14]Section 78 of Information Technology Act, 2000.

It is not talked about regulation of intellectual property rights, particularly copyright on the internet which is an ever-growing problem. The Act does not discuss the implications of any copyright violations over the internet. It has no provisions to penalise copyright infringers, commonly known as 'pirates' for their activities over the internet. Internet piracy is a major problem which has not been tackled by this Act. No amendments have been proposed to the Copyright Act of India.

(f) Cyber Terrorism:- The traditional concepts and methods of terrorism have taken new dimensions, which are more destructive and deadly in nature. In the age of information technology the terrorists have acquired an expertise to produce the most deadly combination of weapons and technology, which if not properly safeguarded in due course of time, will take its own toll. The law dealing with cyber terrorism is, however, not adequate to meet the precarious intentions of these cyber terrorists and requires a rejuvenation in the light and context of the latest developments all over the world. The laws of India have to take care of the problems originating at the international level because the Internet, through which these terrorist carryout all their activities, recognizes no boundaries. Thus, a cyber terrorist can collapse the economic structure of a country from a place with which India may not have any reciprocal arrangements. The only safeguard in such a situation is to use the latest technology to counter these problems. Thus, a good combination of the latest security technology and a law dealing with cyber terrorism is the need of the hour.

In short, we are facing the worst form of terrorism popularly known as "Cyber Terrorism". The expression "cyber terrorism" includes an intentional negative and harmful use of the information technology for producing destructive and harmful effects to the property, whether tangible or intangible, of others. Cyber terrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact.

(g) Less Rate of Conviction:- The absolutely poor conviction rate of cyber crime in the country has also not only helped the cause of regulating cyber crime. There have been few cyber crime convictions in the country, which can be counted on fingers. Government needs to ensure specialized procedures for prosecution of cyber crime cases so as to tackle them on a priority basis. This is necessary so as to win

the faith of the people in the ability of the e-Governance system to tackle cyber crime. Government must ensure that system provides for stringent punishment of cyber crimes and cyber criminals so that the same acts as a deterrent for others. It seems that the Parliament would be required to amend the IT Act, 2000 to remove the grey areas mentioned above.

(h) Ineffectiveness of Cyber Law:- The cyber law, in any country of the World, cannot be effective unless the concerned legal system has the following three prerequisites: i. a sound Cyber Law regime, ii. a sound enforcement machinery and iii. a sound judicial system. Let us analyse the Indian Cyber law on the referred parameters.

i. **Sound Cyber Law Regime:-** The Cyber law in India can be found in the form of Information Technology Act, 2000. Now the IT Act, as originally enacted, was suffering from various lacunas and loopholes. These "grey areas" has been excusable since India introduced the law recently and every law needs some time to mature and grow. It was understood that over a period of time it would grow and further amendments would be introduced to make it compatible with the International standards. It is important to realize that we need "qualitative law" and not "quantitative laws". In other words, one single Act can fulfil the need of the hour. The dedicated law essentially requires a consideration of "public interest" as against interest of few influential segments.[15]

ii. **A Sound Enforcement Machinery:-** A law might have been properly enacted and may be theoretically effective too but it is useless unless enforced in its true letter and spirit. The law enforcement machinery in India is not well equipped to deal with cyber law offences and contraventions. It must be trained appropriately and should be provided with suitable technological support.

iii. **A Sound Judicial System:-** Judiciary is an important part of the government. It plays an important role in the maintenance of law. We know that a sound judicial system is the backbone for preserving the law and order in a society. It is the duty of judges and advocates performing their duty with spirit. This essentially means a rigorous training of the members of both the Bar and the Bench. The fact is that the cyber law is in its infancy stage in India, hence Judges and Lawyers are not much aware about it. Thus, a sound cyber law training of the Judges and

[15]Praveen Dalal, "Cyber Law in India" retrieved from <http://cyberlawsinindia.blogspot.in/2010/06/how-indian-government-made-cyber-law-of.html> access on 20-06-2016.

Lawyers is the need of the hour. In short, the dream for an "Ideal Cyber Law in India" requires a "considerable" amount of time, money and resources.

Conclusion and Suggestions

Technology is very important part of our life and we can't reach at the top without using Electronic Technology in governance. Therefore e-Governance largely depends upon the use of technologies and relating laws of technologies. E-Governance represents new form of governance, which is dynamic and exponential. It needs dynamic laws, keeping pace with the technology advancement. But this is a new dispensation of e-Governance requiring new set of laws to redefine the old structure of governance by meshing with a new structure of the web. E-Governance is about extending the rule of law in cyberspace. Present Information Technology laws fail to cover all aspect of e-Governance.

It is evident from the above discussion that objectives of achieving e-Governance and our ambitions of transforming India go far beyond mere computerization of stand-alone back office operations. It needs fundamental change as to how the government operates, and this implies a new set of responsibilities for the executives and politicians. It will require basic change in our work culture and goal orientation as well as simultaneous change in the existing processes. It will require skilled navigation to ensure a smooth transition from old processes and manual operations to new automated services without hampering the existing services. This can be achieved by initially moving forward with smaller informed initiatives in a time bound manner and avoiding large and expensive steps without understanding the full social implications. The proposed changes may meet with a lot of inertia which cannot be overcome by lower and middle-level officials with half-hearted attempts to diffuse the technology.

On other hand we know that the Information Technology Act, 2000 is suffering from numerous drawbacks and grey areas. Therefore, the amendments must be seen in the light of contemporary standards and requirements. Some of the more pressing and genuine requirements in this regard are:

i. There should be security concerns for e-Governance laws in India.
ii. The use of Information & Communication Technology for justice administration must be enhanced and improved.
iii. The offence of Cyber Extortions must be added to the Information Technology Act, 2000 along with Cyber Terrorism and other contemporary cyber crimes.
iv. The increasing nuisance of website hijacking and hacking must also be addressed.

v. The use of Information & Communication Technology for day to day procedural matters must be considered.
vi. The legal risks of online services in India must be kept in mind at the time of making policy.
vii. Internet banking and its legal challenges in India must be considered.
viii. Adequate and reasonable provisions must be made in the Information Technology Act, 2000 regarding "Internet censorship".
ix. The deficiencies of Indian Information & Communication Technology strategies must be removed and improve as soon as possible.
x. The Government should take seriously the genuine concerns and should avoid the weak cyber legal system in India.
xi. There should be proper authentication of Digital Signature.

Without improving legal system, positive change is not possible in e-Governance. Good governance is need of time and every government has the responsibility to provide it to their citizens. The users of the computer system and the internet are increasing day by day worldwide. In this kind of society where it is easy to access any information easily within a few seconds by using the internet which is the medium for huge information and a large base of communications around the world, certain precautionary measures should be taken by citizens while using the internet which will help in challenging this major threat of Cyber Crimes. Therefore, cyber security must be made strong.