Cyber Security in Digitized E-Governance: Evaluating Indian IT Act 2000 (As Amended in2008) in Context

Alice Dey[1] and Sadhan Kumar Dey[2,*]

[1]*Department of Law, Kalinga University, Raipur, India*

[2]*ESM Dept. RCCIIT, Kolkata, India*

Abstract: Digital technology and Cyber-based database management system in Indian e-governance has brought about dramatic changes in the mode of operations in all governmental business transactions in India. Government organizations and Government professionals need to depend upon the electronic media and computer-generated e-records for e - governance. Information Technology poses new and complex ethical, legal and extra- legal threats to e-governance. This e-governance inter alia involves the question of security against abuses and misuses of Information Technology The situation demands a fresh look into the problem of Cyber Security in e-governance . Information stored in electronic form is cheaper, faster and easier to store, retrieve and to access than traditional paper –based government records. But the question remains:

How far these electronic e-governance records are maintainable in Indian court of law under IT Act 2000 (as amended in 2008)?

Government is aware of the advantages of e-records but is reluctant to conduct or conclude business transactions in the electronic form due to lack of legal framework in India. Globalized technological changes have created a new global economy powered by technology, fuelled by information and driven by the concept of e-governance of the 'government'. The present paper will analyze the challenge of digitized government and will seek answer to the question mentioned above related to Cyber Security in IT- enabled environment of digitized government of India. IT Act 2000 (as amended in 2008) will be critically analyzed and evaluated to find out its efficacy and limitations in ensuring security of e-governance of India.

Keywords: Cyber, Security, digitized, e-governance, evaluating, Indian IT Act 2000.

INTRODUCTION

Database management system in Indian e-governance depends on newly introduced digital technology and Internet-based web tools that have brought dramatic changes in the mode of operations in all business transactions of the government. Government organizations and Government professionals mostly depend upon the electronic media and computer-generated e-records for continuing day to day e – governance of the country. Information technology poses new and complex ethical, legal and extra- legal threats to e-governance both at the Union and Provincial level of India. Day to day gubernatorial affairs of e-governance *inter alia* involves the question of cyber security against abuses and misuses of Information Technology The situation demands a fresh look into the problem of Cyber Security in e-governance of India. Information stored in electronic form is cheaper, faster and easier to store, retrieve and to access than traditional paper –based government record books and ledgers. The present article would focus on the question of cyber security in digitized e-governance of India with reference to the IT Act of India [1].

The present article will answer the question:

How far these electronic e-governance records are maintainable in Indian court of law under the IT Act 2000 (as amended in 2008)?

Though Government officials are aware of the advantages of maintaining e-records yet they are unwilling to conduct day-to-day bureaucratic transactions in the electronic form due to lack of confidence in the legal framework of cyber protection as available in India at present.

The last two decades have reflected the following contemporaneous[1] issues;

i. Globalized technological changes that have created a new global economy

ii. Introduction of ICT [2] in legal studies and judicial documentation

iii. Information Technology fuelled by information and driven by the concept of e-governance for day-today operations and bureaucratic functions of the 'Government of India'.

*Address correspondence to this author at the ESM Dept. RCCIIT, Kolkata, India; E-mail: deysadhan.rcciit@gmail.com

[1]Extending throughout the last century.

In the light of the above issues the present article will analyze the challenge of digitized government and will seek answers to the question mentioned above related to Cyber Security in IT- enabled environment of digitized government of India. IT Act 2000 (as amended in 2008) will be critically analyzed in this context and will be evaluated to find out its efficacy and limitations in ensuring security of e-governance of India.

Information technology poses new and complex ethical, legal and extralegal issues in society which inter alia result in legislative responses due to unwanted uses of Information Technology. Information Technology Act of India like any other Indian law is important to protect the rights of its actual and rightful 'users'. This objective is achieved through enforcing privacy, data protection, validity of online contracts, electronic procurement, data integrity and authenticity, outlining intellectual property rights (IPR) and providing confidence and trust in open systems.

But the phenomenal growth and development in 'Information Technology' and Electronic Media' has got its perks not only by debarring human beings from humane motions but also by making them accountable for certain unethical actions. Most of these are labeled as criminal offences in the computer - generated internet world that are called 'cybercrimes'.

The major pitfalls of this phenomenal growth have given rise to cybercrimes across the globe at an alarming rate. To combat this growing challenge of cybercrimes in India the first legislation came in the year 2000.

Since cyber criminals were found to be a step ahead of misusing the technology with criminal intent, updated amendments became a need of the hour. Even after the introduction of the IT Act of India in 2000 many amendment notifications were issued as per requirement. Legislations so far introduced in India and specially IT (Amendment) Act has provided penal solutions to issues like spamming, phishing, non-integrity of transactions in e-governance[2] of India.

The major challenge remains:

How to incriminate the cyber offenders by using the age –old instrument called Indian Evidence Act, 1872?

The present dissertation has considered all the above issues in line with the futility of Indian Evidence Act, 1872 to examine sustainability of the IT Act of India in regard to admissibility of Electronic[3] Evidence for ascertaining the quantum of possible incrimination of cyber offenders in Cybercrimes in the light of the sustainability of e-governance of India.

CONCEPTUAL FRAMEWORK: IT ACT 2000 (AS AMENDED IN 2008)

Application of Information Technology has provided new ways and means to the offenders of cyber crimes. To counter the threat of growing cyber – crimes the I T Act of India was amended in 2008, Wide ranging cyber crimes were incorporated in this amendment of the act with the provision of financial penalties as well as penal provisions of punishment varying from a three-year jail term to life sentence. This amendment came into force on 29th October, 2009. Broadly IT Act Amendment 2008 has covered following aspects of the said Act with reference to e-governance of India.

i. **Liability of Body Corporate towards Sensitive Personal Data**: Body corporate means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities. Any Body corporate dealing in sensitive personal data or information in a computer resource and lacking in providing sufficient security and control practices to safeguard the data has been made liable under Section 43A to pay damages to the affected party.

ii. **Identity as an Evidence of Theft:** Under section 63 C, Fraudulent or dishonest act by misuse of electronic signature, password or any other a unique identification feature of a person is punishable.

iii. **Spamming and Phishing:** Explicitly no specific law exists against spamming and phishing but it appears that this aspect has been covered under section 66A. It says that sending messages of offensive nature or criminally intimidating through communication service has become punishable with imprisonment for a term which may extend upto three years or with fine.

iv. **Introduction of virus, manipulating accounts, denial of services - made Punishable**: Section

[2]Day to day governance run through the computer network across the country.

[3]Evidence based on computer-generated or network-driven electronic devices.

66 has been amended to include offences punishable as per section 43 which has also been amended to include offences as listed above; punishment may lead to imprisonment which may extend to three years or with fine which may extend to five lakh rupees or with both.

v. **Cyber Terrorism**: intent to threaten the unity, integrity, security or sovereignty of Indiacontributes to cyber terrorism. Section 66D deals with punishment for acts like 'Denial of Services' (DoS) and 'Unauthorized Access' (UA) are related to cyber terrorism.

vi. **Cheating and Stealing of Computer Resource or Communication Device**: Punishment for stealing or retaining of any stolen computer resource or communication devices have been covered under Section 66B. Section 66D makes "cheat by impersonating" by means of any "communication device" or 'computer resource' an offence.

vii. **Intermediary's liability**: Intermediary means any person who on another person's behalf receives stores or transmits the message or provides any service with respect to that message. Sections 67C states that intermediaries should preserve and retain information in the format and for the period given by the Central Government.

viii. **Surveillance, Interception and Monitoring**: Section 69 empowers the government to issue directions for interception or monitoring or decryption of any information through any computer resource.

ix. **Cognizance of cases and investigation of offences**: All cases which entail Punishment of three years or more has been made cognizable. In Act 2000, section 78 defines that investigation of offences is to be done only by the Deputy Superintendent of police. In its amendment, Inspectors have been included as investigating officers which is more feasible.

x. **Security procedures and Practices:** Section 16 empowers the Central Government to prescribe security procedure in respect of secure electronic records and secure digital signatures with reference to e-governance. Electronic governance or e-governance has been adopted by technologically advance countries across the world. Examples of e-governance in India include the following projects and programmes:

- Digital India initiative,
- National Portal of India
- Prime Minister of India portal
- Aadhar, filing and
- Payment of taxes online
- Digital land management systems
- Common Entrance Test

This conceptual framework has shown beyond all reasonable doubts that sustainability of IT Act of India has become a major issue in today's technology–controlled situation in India. Side by side the Indian Evidence Act of 1872 is proved to be inadequate regarding the "Doctrine[4] of Admissibility" of Electronic documents and computers – generated cybercrimes.

DESIGN OF THE STUDY

The present research "Cyber security in digitized E-governance: Evaluating the IT Act 2000 (As Amended in 2008) in context)" is a theoretical research that interalia involves a deeper understanding of It Act 2000 with reference to the Indian Evidence Act,1872.the critical study has been done following the method of descriptive research and theoretical assumptions based on the problems associated with the implementation of IT Act in E-governance in real life situations in India.

The present research paper being a specimen of Doctrinal Research in legal studies has followed the technique and the strategies that are prescribed in legal research.

The general focus of the research design was on critical study of IT Act 2000 which is the core Act for providing guidelines to govern Cyber Laws in India.

The reference point "Electronic Evidence" is the major issue of the present research article. An in-depth study has been taken up to develop a critical study of

[4]It refers to the fact of maintaining the consistent quality of being authentic and unchanged in its version every time the document is produced in any law court of India.

comparative analysis of the governance of the IT Act 2000 in trade and commerce, in business and in the E-Governance of the country. The current scenario of State governments and the Central Governments too are guided by IT Laws and Cyber Laws with reference to both internal governance of the State and the external foreign policy of India as well as inter-state relationships.

DIGITIZED E-GOVERNANCE AND INFORMATION TECHNOLOGY ACT 2000 (AS AMENDED IN 2008)

From the perspective of e - Governance in India, the IT Act 2000 and its provisions contain many positive aspects. They are as discussed below:

a) In the first place the implication of these provisions for e- Governance is that e-mail is now a valid and legal form of communication in India that can be duly produced and approved in a court of law.

b) Companies are now able to carry out electronic commerce using the legal infrastructure provided by the Act.

c) Digital signatures have been given legal validity and sanction in the Act.

d) The Act[5] opens the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signature Certificates.

e) The Act now allows the Government to issue notification on the web thus heralding e-governance in India.

f) The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.

g) The IT Act also addresses the important issues of security, which are critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to be passed through a system of a security procedure, as stipulated by the Government at a later date notification.

Under the IT Act, 2000, it is possible for corporate and Government organizations to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding Rs. 5 Crores. This research work would judge the sustainability of the Act in the light of all associate Laws prevalent in India. This is enough to provide background and rationale of the present dissertation.

REVIEWING OPERATIONAL ASPECTS OF CYBER SECURITY IN E-GOVERNANCE

Electronic Evidence is the means by which facts relevant to the guilt or the innocence of an individual at trial is established. Electronic evidence is all such material that exists in electronic, or digital, form. Electronic evidence is central not only to the investigation and prosecution of forms of cybercrime, but increasingly to crime in general. Legal frameworks optimized for electronic evidence, together with law enforcement and criminal justice capacity to identify, collect and analyze Electronic evidence is thus central to an effective crime response. Generating

Evidence like user interaction with computer devices produces a wealth of computer-generated digital traces often called digital fingerprints or artifacts. It considers the criminal justice process in cybercrime cases, starting from the need to identify, collect and analyze the computer generated evidence through digital forensics. It examines the admissibility and use of electronic evidence in criminal trials, and demonstrates how a range of prosecutorial challenges can impact on criminal justice system performance. It links law enforcement and criminal justice capacity needs with a view of delivered and required technical assistance activities.

Electronic communications potentially relevant to a criminal act may include gigabytes[6] of photographs, videos, emails, chat logs and system data. Locating relevant information within this data can be extremely time-consuming. The variety of possible file formats [3], operating systems, application software, and hardware

[5]Information Technology Act of India 2000 (as amended in 2008).

[6]Units of digitized information equal to one thousand million (10^9) or, strictly, 2^{30} bytes.

particulars also serves to complicate the process of identifying relevant information. Computer artifacts can be easily modified, overwritten or deleted, thus posing challenges where sources of digital information must be authenticated and verified[7]. Evidence rules vary considerably between jurisdictions, even amongst countries with similar legal traditions.

In general terms, however, legal systems of the common law tradition tend to have defined rules as to the admissibility of evidence. In legal systems of the civil law tradition, in which professional judges retain a high degree of control over the court proceedings, admissibility of evidence may be flexible, although the weighing of evidence including ascertaining its credibility and authenticity can also obey a comprehensive set of rules. In many legal systems across the globe the quality of procedures applied to maintain the integrity of digital information from the moment of creation to the point of introduction in court must be demonstrated by the proponent of the evidence. The integrity and authenticity of digital information has a direct bearing on the weight of evidence, in terms of its reliability and trustworthiness. The party seeking to introduce evidence must usually demonstrate evidence continuity, or 'chain-of-custody,' so that it can be proved that the evidence has not been tampered with or otherwise altered. Evidence continuity is typically a question of fact and the chain-of-custody process is the mechanism applied for maintaining and documenting the chronological history of the evidence as it moves from one place to another.

The reliability of computer-generated and computer-stored information has also been challenged on the basis of security vulnerabilities in operating systems and programs that could give rise to threats to the integrity of digital information. The susceptibility of digital information to manipulation has been considered by courts when introducing electronic evidence, with emphasis on 'the need to show the accuracy of the computer in the retention and retrieval of the information at issue. In addition to demonstrating authenticity and integrity of evidence, challenges to the use of electronic evidence arise, in some jurisdictions, from the application of particular evidential rules. Digital forensics is the branch of forensic science concerned with the recovery and investigation of material found in digital and computer systems.

[7]Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors

Section 4 of the IT Act provides that where any law provides that information or any other matter shall be in writing, then, such requirement shall be deemed to have been satisfied if such information or matter is made available in electronic form and is available for use for a subsequent reference. In order to ensure that electronic records are authentic the Act provides for authentication of electronic records by affixing a Digital Signature by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record. In 2008 section 3A was inserted into the IT Act which allows for other means of authenticating electronic records.

The IT Act also made a number of amendments to the Indian Evidence Act which are specified in the Second Schedule to the IT Act so as to enable production of electronic records as evidence in courtroom proceedings.

EVIDENTIARY NEED AND THE INTERNET PROTOCOL

Let us outline the issues involved in applying Indian law of evidence to the Internet. It uses for basic reference the Indian Evidence Act, 1872 and the Information Technology Act, 2000. Passing references are also made to legislation and practice of advanced countries of the world.

Computer-generated electronic evidence are taken to be valid evidence in almost all law courts in India. This is primarily because technology today only allows for Internet usage through computers and mobile technology. It is necessary to have the definition of what a 'Computer' is as referred to in IT Act. Section 2(1) (i) of the IT Act defines a computer as "… any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network". However, technology is fast embracing mobile technology, where users can access the Internet, use Email, send and receive faxes, etc, by mobile phones through the Wireless Application Protocol (WAP). Also, the mushrooming industry is Internet Service through television and cable companies.

Either way, all of this communication involves processing the transaction through a mechanical

device**.** It is true that the Indian Evidence Act1872 does not define a computer, but allows for "copies" to be made by mechanical processes", or through uniformly "printing". References to "computer" and "media" are also taken to be evidence in the Companies Act 1956. It is interesting to note the fact that [4] for the purposes of the Companies Act, it is not necessary for the *computer* to be working properly.

The only mechanical device that needs to be checked for functional problems is the *media* where such data are stored in. In the United Kingdom, it is necessary to prove the computer was working properly before adducing computer-generated evidence.

This gives rise to the first problem as regards Internet-based evidence. For example, *X* in an Email to *Y* confirmed that he accepted *Y's* offer, thereby concluding a contract. *Y* accessed his E-mail account and directly downloaded X's Email onto a diskette. The Email did not pass through the computer *Y* was using [4], but a virus piggybacked onto the file while saving had occurred and, thereby, changed the content of the source E-mail. Now, all that has to be proved to admit this tampered E-mail (for the purposes of the Companies Act), is that the diskette (media on which the data was stored) was functioning properly.

As a matter of fact the IT Act has defined computers and has also focused on Internet-based crimes that are governed under cyber laws. But there are no such guidelines regarding the functionality of the computer concerned when some evidence is computer generated and mechanically processed and is available in uniform printing.

ADMISSIBILITY OF ELECTRONIC RECORDS

"Electronic Record" refers to data, record or data generated, image or sound sorted, received or sent in an electronic form or microfilm or computer generate microfiche fiche [5]. The new amendments made in the Indian Penal Code,1860 states that all the offences related to "documents" shall also include offences related to 'electronic records' which are committed through cyberspace or the Internet.

There are in all twenty IPC offences wherein the use of the word "document" shall also include "electronic record". Some are as follows:

- Offences by or relating to public servants (Sec.167, IPC)
- Absconding to avoid service of summons to produce electronic record (Sec.172)
- Fabricating False evidence/ electronic evidence(Sec.192)
- Forging certain documents /records (Sec.463)
- Falsifying accounts (Sec.477-A)
- Criminal Intimidation (Sec.503)

Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer shall be deemed to be a document. If the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

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

- 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 fed into the computer in the ordinary course of the said activities;
- Throughout the material part of the 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 that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and
- The information contained in the electronic record reproduces such information fed into the computer in the ordinary course of the said activities.

Where the information was processed or fed into the computer on inter-linked computers or one computer after the other in succession, all the computers so used shall be treated as one single

computer. The references to a computer have to be construed accordingly.

CONCLUSION

In the case of digital information, evidence continuity must be maintained for both the physical device housing the data when received or seized, and the stored data residing on the device [6] As such, the party offering the evidence must demonstrate that:

(i) the digital information obtained from the device is a true and accurate representation of the original data contained on the device (authenticity); and

(ii) that the device and data sought to be introduced as evidence is the same as that which was originally discovered and subsequently taken into custody (integrity).

The objective is to show that the device is what it is purported to be and that the digital information is trustworthy, and has not been tampered with or altered.

The issue of cyber security and surveillance, especially unauthorized surveillance, though traditionally semi-prioritized, has recently gained much attention due to the increasing number of news reports regarding various instances of unauthorized surveillance and cyber crimes.

In India the Information Technology Act, 2000 was passed as a law addressing digital content and to grant legal recognition to transactions carried out by means of electronic communication.

Thus, with this amendment to the Evidence law. An electronic document can for all practical purposes have the same legal effect as a paper based original document so long as the conditions mentioned in sub-clauses (a) to (d) of clause (2) of the amended section are satisfied.

Thus, we see that the question of Cyber Security can never be resolved through stringent laws and application of Artificial Intelligence and advanced Computing in Cyber Forensic Lab.

The more stringent punitive measures taken for controlling Cyber Crime may lead to desperate and ferocious misuse of Digitized Platform as is noticeable in the efforts of spreading Cyber Terrorism all over the world. The time has come to look within and forge ahead with “Right Understanding” and “Right Feeling” to utilize the Digitized Revolution for maintaining holistic vision for mutual happiness in human-human relationship and for ensuring mutual prosperity in relation to Nature and Existence.

REFERENCES

[1] Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. New York: Elsevier 2011.

[2] Koops BJ. The Internet and its Opportunities for Crime. In: Herzog-Evans M, (Ed.) Transnational Criminology Manual. Nijmegen, Netherlands: WLP 2010. https://doi.org/10.2139/ssrn.1738223

[3] Jackson JD, Summers SJ. The Internationalisation of Criminal Evidence: Beyond the Common Law and Civil Law Traditions. Cambridge: Cambridge University Press 2012. https://doi.org/10.1017/CBO9781139093606

[4] Marcella Jr. AJ, Greenfield RS, (Eds.). Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2nd edition Boca Raton: CRC Press 2002; p. 136. https://doi.org/10.1201/9781420000115

[5] Information Technology (ITT) Act 2000 (as amended in 2008 (https://police.py.gov.in/Information%20Technology%20Act%202000%20-%202008%20(amendment).pdf)

[6] U.S. Department of Justice. Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors. National Institute of Justice 2007; p.16.

Received on 10-12-2022 Accepted on 05-01-2023 Published on 04-02-2023