International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 1, pp: 1259-1262 www.ijaem.net ISSN: 2395-5252

Cyber Law and Digital Evidence in India

Dr.Sairam Patro
Guest Faculty, Lingaraj Law College, Berhampur University, Berhampur, Odisha

Date of Submission: 01-07-2020 Date of Acceptance: 16-07-2020

ABSTRACT
Cyber law encapsulates the legal issues related to use of communicative, transactional and distributive aspects of networked information devices and technologies. The Indian Evidence system earlier relied heavily on paper documents and oral testimony. The development of e-commerce and digital technology where electronic devices came to be used instead of papers and manuscripts, the proliferation of computers, the social influence of information technology and the ability to store information in digital form have all necessitated a change in the system, which in turn required Indian law to be amended to include provisions on the appreciation of digital evidence. Digital evidence can relate to online banking frauds, online share trading fraud, source code theft, credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, divorce cases, murder cases, organized crime, terrorist operations, defamation, pornography, extortion, smuggling etc. The judiciary in India is not only aware of the advantages of information technology but is actively and positively using it in the administration of justice, particularly the criminal justice.

Keywords: *Cyber Law, Digital Evidence, IT Act, 2000, E-governance, E-commerce*

I. INTRODUCTION

The evolution of information technology gave birth to the cyber space[1]. Cyber space is a very wide term and includes computers, networks, software, data storage devices (such as hard disks, USB disks etc), the Internet, websites, e-mails and even electronic devices such as cell phones, ATM machines etc. It is governed by a system of law and regulation called cyber law. In today's highly digitalized world cyber law affects almost everyone. Cyber law can be defined as the law governing computers and the internet. It encapsulates the legal issues related to use of communicative, transactional and distributive aspects of networked information devices and technologies. In general, Cyber law encompasses laws relating to:

1. Cyber Crimes
2. Electronic and Digital Signatures
3. Intellectual Property Rights
4. E-governance
5. E-commerce
6. Data Protection and Privacy

Cyber crimes are unlawful acts where the computer is used either as a tool or a target or as an accessory to store illegal or stolen information. The enormous growth in electronic commerce (e-commerce) and online share trading has led to a phenomenal spurt in incidents of cyber crime.

Technological Developments and the Law of Evidence

Evidence is the most important thing before a court of law. It must be something that the court can rely upon and based on which it can arrive at its findings either for conviction or acquittal or deciding on damages. The requirement of law is that evidence must be of such amplitude as warranted the seriousness of the offence for awarding the sentence. However, the Courts are often called upon to deal with complex cases relating to highly sophisticated crimes where criminals take care to erase all evidence of their involvement.

The Indian Evidence Act 1872 introduced a standard set of law applicable to all Indians. The main principles which underlie the law of evidence are: (1) Evidence must be confined to the matter in issue; (2) Hearsay evidence must not be admitted; and (3) Best evidence must be given in all cases.

The Indian Evidence system earlier relied heavily on paper documents and oral testimony. The development of e-commerce and digital technology where electronic devices came to be used instead of papers and manuscripts, the proliferation of computers, the social influence of information technology and the ability to store information in digital form have all necessitated a change in the system, which in turn required Indian law to be amended to include provisions on the appreciation

[1]. Singh, Ranbir and Singh Ghanshyam (Eds); Cyber Space and the Law-Issues and Challenges (Hyderabad 2004)

International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 1, pp: 1259-1262 www.ijaem.net ISSN: 2395-5252

of digital evidence. At the international level the United Nations Commission on International Trade Law Model Law (UNCITRAL) had adopted a Model Law in 1996. In order to conform to the UNCITRAL Model Law of 1996, and meet the requirements arising out of the rapid technological developments, the Information Technology Act was adopted in 2000. The Act amended the existing Indian Statutes to allow for the admissibility of digital evidence. The IT Act is based on the on Electronic Commerce and together with providing amendments to the Indian Evidence Act 1872, the Indian Penal Code 1860 and the Banker's Book Evidence Act 1891; it recognizes transactions that are carried out through electronic data interchange and other means of electronic communication.

Digital Evidence

Digital Forensic Evidence consists of exhibits, each consisting of a sequence of bits, presented by witnesses in a legal matter, to help the court to establish the facts of the case and support or refute legal theories of the case. It is information of probative value that is stored or transmitted in a binary form, which a party to a court case may use at trial[2].

Digital evidence can relate to online banking frauds, online share trading fraud, source code theft, credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, divorce cases, murder cases, organized crime, terrorist operations, defamation, pornography, extortion, smuggling etc. Digital evidence can relate to online banking frauds, online share trading fraud, source code theft, credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, divorce cases, murder cases, organized crime, terrorist operations, defamation, pornography, extortion, smuggling etc.

The Information Technology Act 2000

To meet the challenges posed by the information technology, the Parliament has enacted the Information Technology Act, 2000[3]. The IT Act has been based largely on the UNCITRAL Model Law on Ecommerce. At present the primary source of cyber law in India is the Information Technology Act, 2000. The objectives of the Act are to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government; to provide a sound base for e-governance and e-commerce by giving legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code,1860, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

The Act stipulates numerous provisions in order to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The Act further states that unless otherwise agreed to, the acceptance of a contract expressed by electronic means of communication shall have legal validity and enforceability. The Act would facilitate electronic intercourse in trade and commerce, eliminate barriers and obstacles to electronic commerce that result from the celebrated uncertainties relating to writing and signature requirements over the Internet. The objectives of the Act also aim to promote and develop the legal and business infrastructure necessary for implementing electronic commerce.

The Supreme Court's stress on creative interpretation to enable the judiciary to respond to Technological Developments.

In *State of Punjab v Amritsar Beverages Ltd*[4], the Apex Court stressed on the need for creative interpretation so that the judiciary can respond to technological developments. The case involved a search by the Sales Tax Department and the seizure of computer hard disks and documents from the dealer's premises. The computer hard disk was seized under the provisions set out in Section 14 of the Punjab General Sales Tax Act 1948, which requires authorities to return seized documents within a stipulated time frame Section 14 (3), provided that the dealer or person concerned is given a receipt for the property.

i. Tape recordings:

In 1975, the Supreme court of India in the case of *ZiyauddinBurhanuddinBukhari v. BrijmohanRamdassMehra*[5] has observed that tape

[2] Casey, Eoghan (2004). Digital Evidence and Computer Crime, Second Edition.
[3]. The Act came into force on 17 October 2000
[4]. *2006 IndLawSC 391*
[5]. *AIR 1975 SC 1788*

recorded speeches constitute a document as defined by section 3 of the Evidence Act, which stand on the same footing as photographs, and they are admissible in evidence on satisfying the conditions (1.)the voice of the person alleged to be speaking must be duly identified by the maker of the record or by others who knew it; (2) accuracy of what was actually recorded had to be proved by the maker of the record and satisfactory evidence, direct or circumstantial, to rule out possibilities of tampering with the record had to be presented; (3)the subject matter recorded had to be shown to be relevant according to the rules of relevancy found in the Evidence Act.

ii. Examination of a witness by video conference

In *State of Maharashtra v Praful B. Desai*[6] the Supreme Court opined that actual physical presence is not a must and a person would be able to present himself through "video conferencing" in presence of his pleader, and the same can be considered as evidence. It was also stated by the court that the evidence can also be recorded through "video conferencing", and the same would be authentic. The Supreme Court observed that video conferencing is an advancement of science and technology which permits seeing, hearing and talking with someone who is not physically present with the same facility and ease as if they were physically present. The legal requirement for the presence of the witness does not mean actual physical presence. The court allowed the examination of a witness through video conferencing and concluded that there is no reason why the examination of a witness by video conferencing should not be an essential part of electronic evidence.

iii. **Admissibility of intercepted telephone calls**

In *State (NCT of Delhi) v. NavjotSandhu, SAR Gilani&Ors*[7] there was an appeal against conviction following the attack on Parliament on December 13, 2001. The facts were that five heavily armed persons entered the Parliament House Complex and killed nine people, including eight security personnel and one gardener, and injured 16 people, including 13 security men. This case dealt with the proof and admissibility of mobile telephone call records. While considering the appeal against the accused for attacking Parliament, a submission was made on behalf of the accused that no reliance could be placed on the mobile telephone call records, because the prosecution had failed to produce the relevant certificate under Section 65B(4) of the Evidence Act. The Supreme Court held that it is not in dispute that the information contained in the call records is stored in huge servers which cannot be easily moved and produced in the Court. That is what the High Court has also observed at para 276. Hence, printouts taken from the computers/servers by mechanical process and certified by a responsible official of the service providing Company can be led into evidence through a witness who can identify the signatures of the certifying officer or otherwise speak to the facts based on his personal knowledge. The Supreme Court concluded that a cross-examination of the competent witness acquainted with the functioning of the computer during the relevant time and the manner in which the printouts of the call records were taken was sufficient to prove the call records. The apex court while examining the provisions of Section 65B held that in a given case, it may be that the certificate containing the details in sub-section 4 of section 65B is not filed, but that does not mean that secondary evidence cannot be given. It was held by the court that the law permits such evidence to be given in the circumstances mentioned in the relevant provisions of the Indian Evidence Act 1872. Irrespective of the compliance of the requirements of Section 65B which is a provision dealing with admissibility of electronic records, there is no bar to adducing secondary evidence under the other provisions of the Evidence Act, namely Sections 63 and 65.Above all, the printouts pertaining to the call details exhibited by the prosecution are of such regularity and continuity that it would be legitimate to draw a presumption that the system was functional and the output was produced by the computer in regular use, whether this fact was specifically deposed to by the witness or not. The Supreme Court concluded that a cross-examination of the competent witness acquainted with the functioning of the computer during the relevant time and the manner in which the printouts of the call records were taken was sufficient to prove the call records.

Paragraph 150 of the judgment which is apposite, reads as under: "According to Section 63, secondary evidence means and includes, among other things, "copies made from the original by mechanical processes which in themselves insure the accuracy of the copy, and copies compared with such copies. Section 65 enables secondary evidence

[6]. *AIR 2003 SC 2053; 2003 AIR SCW 1885.*
[7]. *State (NCT of Delhi) v NavjotSandhu, (2005) 11 SCC 600, AIR 2005 SC 3820, 2005 Cri LJ 3950, 122 (2005) DLT 194(SC).*

of the contents of a document to be adduced if the original is of such a nature as not to be easily movable. Hence, printouts taken from the computers/servers by mechanical process and certified by a responsible official of the service-providing company can be led in evidence through a witness who can identify the signatures of the certifying officer or otherwise speak of the facts based on his personal knowledge. Irrespective of the compliance with the requirements of s 65-B, which is a provision dealing with admissibility of electronic records, there is no bar to adducing secondary evidence under the other provisions of the Indian Evidence Act 1872, namely, Sections 63 and 65."

iv. SMS as admissible evidence

One of the pieces of circumstantial evidence sought to be relied by the prosecution in the PramodMahajan Murder Trial, was a threatening SMS (Short Message Service) sent by PravinMahajan (the accused) to PramodMahajan. The defense, (a) gave a demonstration that a SMS could emanate from a particular handset/mobile number and when received could display another mobile number; (b) referred to certain provisions of the Indian Evidence Act, 1872 and stated that the SMS was inadmissible as evidence in Trials since, "only secured electronic evidence could be accepted as valid evidence.

On an interesting note, the Hon'ble Judge dismissed the defense contentions on the grounds that (a) the practical demonstration was conducted by defense witness, P Balakrishnan, on a Motorola handset similar to that of Pramod, but not Pramod's phone; and (b) Balakrishnan was "not an expert" as per law as he doesn't have the authorized qualifications.

v. Place of receipt of e-mail

In*M/s. P. R. Transport Agency v. Union of India*[8] the Allahabad High Court held that the acceptance of the tender, communicated by the respondents to the petitioner by e-mail, will be deemed to be received by the petitioner at Varanasi or Chandauli, which are the only two places where the petitioner has his place of business.

II. CONCLUSION

The advent of information technology has changed the mode of working of almost all the spheres of the life. The justice delivery system has also been benefited by this technological revolution. It must be noted that one of the cardinal rule of interpretation is that the Parliament intends the Courts to apply to an ongoing Act a construction that continuously updates its wordings to allow for changes since the Act was initially framed.

With the passage of the Information Technology Amendment Act 2008, India has become technologically neutral due to adoption of electronic signatures as a legally valid mode of executing signatures. This includes digital signatures as one of the modes of signatures and is far broader in ambit covering biometrics and other new forms of creating electronic signatures. ITA 2008 not only defined "Cyber Security" as a part of the legislation, it also introduced the concepts of "Reasonable Security Practices" to be followed by the industry to protect "Data". It also expanded the list of Cyber Crimes covered, strengthened the institution of the Cyber Regulations Appellate Authority (Now called Cyber Appellate Authority), introduced the concept of "Electronic Signatures" and e-auditing.. It expanded the powers of the adjudicators and at the same time also brought the judiciary into the system of civil suits involving Cyber crimes. The rules under sections 69, 69A and 69B have provided enormous powers to the executive for Privacy invasion but have also made the issue of "Cyber Law Compliance" a critical issue in the industry.

The judiciary in India is not only aware of the advantages of information technology but is actively and positively using it in the administration of justice, particularly the criminal justice.

Unlike tangible evidence such as fingerprints, digital evidence presents a new challenge for today's judges to overcome.

Indian courts have responded fairly well to the challenge that the digital evidence has thrown. The legal community has recognized the significant evidentiary role that computers play in civil and criminal cases. Some of the important computer forensic case law in both criminal and civil cases includes cases dealing with email investigations, deleted data etc.

[8]. *AIR 2006 Allahabad 23.*

International Journal of Advances in Engineering and Management
ISSN: 2395-5252

IJAEM

Volume: 02 Issue: 01 DOI: 10.35629/5252

www.ijaem.net
Email id: ijaem.paper@gmail.com