

DON BOSCO INSTITUTE OF TECHNOLOGY, MUMBAI - 400 070
Department of Computer Engg. & Info. Technology
(Academic Year ODD Semester 2021 – 2022)

Course Code and Name: ILO 7016 - Cyber Security and Laws (BE Sem VII)

Name: Hayden Cordeiro

Branch: Comps

Roll no: 05

ASSIGNMENT NO 5

Assignment Questions:

1. Explain the liability aspect of the Internet Service Provider as per the Information Technology Act 2000.

- Chapter XII of the Act provides for issues regarding the liability of the service providers. The Act refers to ISPs as 'network service providers' and exempts them from their liability.
- Section 79 absolves the ISP's liability if they can prove they had no knowledge about the infringement or due diligence was exercised for prevention of such acts.
- The Indian position in liability of service providers for copyright infringement must be made more explicit.
- The Act must include sections that address the financial aspect of the transaction, and the relationship between an ISP and a third party, because this is vital to determining the identity of the violator.
- The American concept of contributory infringement can also be incorporated into the Indian Act so that if any person with knowledge of the infringing activity, induces, causes, or materially contributes to the infringing conduct of another, the person can be made liable.
- In order to be exempt from liability, the Indian Act requires the service provider to exercise due diligence to prevent the commission of copyright infringement.
- The Act does not provide the meaning of the term due diligence. If due diligence means policing each and every aspect of the internet, it can lead to loss of privacy and can ultimately have a disastrous effect.
- There is a need for a consensus on the meaning of the term due diligence because the primary function of ISPs is to build the internet, not to play the role of a policeman.
- If the behaviour of an ISP is reasonable, then that ISP should not be held liable for each and every activity on the internet as has been held by the US courts.

2. Write the salient features of Information Technology Act, 2000.

- All electronic contracts made through secure electronic channels are legally valid.
- Legal recognition for digital signatures.
- Security measures for electronic records and also digital signatures are in place
- A procedure for the appointment of adjudicating officers for holding inquiries under the Act is finalized
- Provision for establishing a Cyber Regulatory Appellant Tribunal under the Act. Further, this tribunal will handle all appeals made against the order of the Controller or Adjudicating Officer
- An appeal against the order of the Cyber Appellant Tribunal is possible only in the High Court
- [Digital Signatures](#) will use an asymmetric cryptosystem and also a hash function
- Provision for the appointment of the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities. The Controller to act as a repository of all digital signatures.
- The Act applies to offences or contraventions committed outside India
- Senior police officers and other officers can enter any public place and search and arrest without warrant
- Provisions for the constitution of a Cyber Regulations Advisory Committee to advise the Central Government and Controller.

3. Explain the various forms of economic offences in India.

Economic offences in India can be classified into three categories. These categories of economic offences are:

- (i) Traditional economic crime which includes corruption, smuggling, bogus imports etc.
- (ii) Emerging technological economic crimes that include credit card frauds, counterfeiting, cyber crimes etc.
- (iii) Crimes through which proceeds of transnational organized crime are transmitted abroad like money laundering.

These categories of crimes include certain crimes that are described as under:

- **Corruption:** – Corruption is a kind of economic offence that is tributed to be a country's primary reasons for low as well as slow economic development as well as a major contributor for the existing poverty in India. The basic reason for corruption is greed. The reasons behind the exponential rate of increase in corruption are monopolies of an individual or a party, power and discretion without accountability.
- **Smuggling:** – Smuggling consists of clandestine operations leading to unrecorded trade, and is one of the major economic offences that is affecting India. Although it is impossible to measure the exact amount of goods smuggled in India, it won't be wrong to say that smuggling occurs at such a level that it forms a major part of the total economic offences that are committed. Smuggling in its broader sense even includes drug trafficking, smuggling of migrants and trafficking of persons.

- **Invoice Manipulation:** – This is another kind of economic offence that affects not only India but all the developing countries severely. Invoice manipulation basically means invoicing a good at a price lower or higher than the price for which it was actually sold or purchased. This kind of transaction mostly happens between trade partners. The person involved in this kind of crime is considered to be guilty of fabricating false documents and records. This kind of economic offence affects the economic position of a country.
- **Bogus Imports:** – This kind of economic offence indicates that there is leakage of foreign exchange through the device of bogus imports. The modus operandi is quite simple. The operator opens a current account in India in a bank authorized to deal in foreign exchange. He usually poses as a small-scale industrialist and produces forged certificates/documents to establish his credentials. His partners abroad prepare a set of export documents such as an invoice, bill of lading, and bill of exchange and send them through their foreign bank branches to Indian banks for collection. Upon receipt of these documents, generally on collection basis, the importer's agent deposits the amount in Indian rupees in his bank's current account and the bank remits the foreign exchange. No goods, of course, are ever imported and the country loses the valuable foreign exchange.
- **Cyber Crimes:** – With the increase of technology and computer usage it is not a surprise that such technology is used for the commission of economic offences. These crimes include theft of computer services, unauthorized access to protected computers, software piracy etc. Cybercrimes have become a reality of today's world in such a manner that today's cyber hackers break into and maliciously alter the content of several computer websites.
- **Counterfeiting:** – Currency counterfeiting is an organized white-collar crime, which is undertaken at alarming rates globally. It not only causes serious setbacks to the world's economy but also jeopardizes genuine business transactions. These days, counterfeiting of currency notes is done with the help of modern equipment. Counterfeiting, however, goes beyond the production of bogus currency to the counterfeiting of all kinds of manufactured products such as clothing, audio and video equipment, compact discs, watches, liquor, perfumes, etc. In such cases, losses are suffered by the manufacturers of the products, their employees, the economies of the concerned states and the concerned governments that would have received tax revenues.
- **Credit Card Frauds:** – As financial institutions introduce innovations against counterfeiting and fraud, increasingly sophisticated ways of profiting from or beating those systems are devised. Most of the credit card fraud is committed by using counterfeited cards, which are pre-embossed or re-encoded.
- **Money Laundering:** – Globalization has brought in the transfer of money globally. The rapid growth of international financial activities takes advantage of political borders and exploits the differences between legal systems in order to maximize profits. Money laundering is another massive contributor to economic offences like corruption. Laundering operations are intended to conceal the origin of the money rather than in the creation of wealth directly, in other words, to hide the traffic from which it is derived rather than the general criminal activity which actually generated it. It is therefore essential to move the money in order to scramble the route it takes. The operation is wholly successful when the nature of the money is also concealed and it is impossible to establish a link with any criminal activity because the different circuits have taken to give it the appearance of legitimate income

4. Briefly explain the scope of cyber law in India with reference to Information Technology Act, 2000.

- India enacted the Information Technology Act, 2000 ("IT Act") on 09 June 2000. The IT Act now becomes the law of land in India which in general terms is also known as Cyber Law.
- The IT Act is based on the UNCITRAL model law on e-commerce
- The preamble of the IT Act simply indicates that the Act is centered on affording legal recognition to transactions carried out electronically.
- However, the scope of the IT Act goes much beyond its preamble.
- It covers multiple areas including data protection and security, cybercrimes, adjudication of cyber disputes, government mandated surveillance of digital communication, and intermediary liability.
- The following Act, Rules, and regulations are included under cyber laws.
 1. Information Technology Act, 2000
 2. Information Technology (Certifying Authorities) Rules, 2000
 3. Information Technology (Security Procedure) Rules, 2004
 4. Information Technology (Certifying Authority) Regulations, 2001
 5. The Indian Evidence Act, 1872
 6. The Bankers Books Evidence Act, 1891
- Emerging technologies, explosion of digital business models and a substantial increase in the instances of cybercrimes have triggered the government to take steps to fast track the process of amending the IT Act.
- In a cyber-crime, computer or the data itself is the target or the object of offence or a tool in committing some other offence, providing the necessary inputs for that offence. All such acts of crime will come under the broader definition of cyber-crime.
- Cyber law encompasses laws relating to:
 - Cyber crimes
 - Electronic and digital signatures
 - Intellectual property

- Data protection and privacy

5. Explain the UNCITRAL model law on electronic commerce. Purpose

The Model Law on Electronic Commerce (MLEC) purports to enable and facilitate commerce conducted using electronic means by providing national legislators with a set of internationally acceptable rules aimed at removing legal obstacles and increasing legal predictability for electronic commerce. In particular, it is intended to overcome obstacles arising from statutory provisions that may not be varied contractually by providing equal treatment to paper-based and electronic information. Such equal treatment is essential for enabling the use of paperless communication, thus fostering efficiency in international trade.

The MLEC was the first legislative text to adopt the fundamental principles of non-discrimination, technological neutrality and functional equivalence that are widely regarded as the founding elements of modern electronic commerce law. The principle of non-discrimination ensures that a document would not be denied legal effect, validity or enforceability solely on the grounds that it is in electronic form. The principle of technological neutrality mandates the adoption of provisions that are neutral with respect to technology used. In light of the rapid technological advances, neutral rules aim at accommodating any future development without further legislative work. The functional equivalence principle lays out criteria under which electronic communications may be considered equivalent to paper-based communications. In particular, it sets out the specific requirements that electronic communications need to meet in order to fulfil the same purposes and functions that certain notions in the traditional paper-based system - for example, "writing," "original," "signed," and "record"- seek to achieve.

Key provisions

Besides formulating the legal notions of non-discrimination, technological neutrality and functional equivalence, the MLEC establishes rules for the formation and validity of contracts concluded by electronic means, for the attribution of data messages, for the acknowledgement of receipt and for determining the time and place of dispatch and receipt of data messages.

It should be noted that certain provisions of the MLEC were amended by the Electronic Communications Convention in light of recent electronic commerce practice. Moreover, part II of the MLEC, dealing with electronic commerce in connection with carriage of goods, has been complemented by other legislative texts, including the United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea (the "Rotterdam Rules") and may be the object of additional work of UNCITRAL in the future.

Additional information

The Model Law is accompanied by a Guide to Enactment, which provides background and explanatory information to assist States in preparing the necessary legislative provisions and may guide other users of the text.

The [CLOUT \(Case Law on UNCITRAL Texts\)](#) system contains cases relating to the application of the Model Law on Electronic Commerce


6. Explain the role and functions of the certifying authorities in e- governance.

Functions of CCA (Secs. 18-25)

- ❖ To act as regulator of certifying authorities (Sec. 18).
- ❖ The main functions of the controller are to regulate the working of certifying authorities. He performs the following functions in this regard:
 - ❖ To exercise supervision over the activities of CAs
 - ❖ To certify public keys of CAs
 - ❖ To lay down the standards to be maintained by CAs
 - ❖ To specify the qualifications and experience for employee of CAs
 - ❖ To specify the conditions for conducting business by CAs
 - ❖ To specify the terms and manner for maintenance of accounts by CAs
 - ❖ To specify the terms and conditions for appointment of auditors and their remuneration
 - ❖ To facilitate the establishment of any electronic system as well as regulation of such system
 - ❖ ➤
 - ❖ To specify the manner of conducting dealings by CAs with the subscribers
 - ❖ ➤
 - ❖ To resolve any conflict of interest between CAs and the subscribers
 - ❖ ➤
 - ❖ To lay down the duties of CAs
 - ❖ ➤
 - ❖ To maintain database for every CA containing their disclosure record as well as such particulars as may be specified by regulations, which shall be accessible to public.
 - ❖ To recognise the foreign certifying authority (Sec. 19).
 - ❖ The controller, with the prior permission of the Central Government and by notification in the Official Gazette, may recognise any foreign certifying authority for the purpose of this Act [Sec. 19(1)].

- ❖ The controller may revoke such recognition by notification in the Official Gazette for reasons to be recorded in writing [Sec. 19(3)].
- ❖ To grant licence to CAs to issue electronic signature certificate (Sec. 21). The controller can grant a licence to any person to issue electronic signature certificate provided he applies and fulfils such requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities which are necessary for the issue of Electronic Signature Certificate [Sec. 21(1) and (2)].
- ❖ The controller may after considering the documents and such other factors, as he deems fit, grant the licence or reject the application. He may reject only after the applicant has been given a reasonable opportunity of presenting his case (Sec. 24).
- ❖ To suspend licence (Sec. 25).
- ❖ The controller may suspend licence if he is satisfied after making an enquiry that CA has:
 - ❖ made a statement which is incorrect or false in material particulars in or relation to the application for the issue or renewal of licence.
 - ❖ failed to comply with terms and conditions necessary for granting of licence.
 - ❖ failed to maintain standards specified in Sec. 30.
 - ❖ contravened any provisions of the Act, rule, regulation or order made thereunder.
- ❖ The notice of suspension or revocation may be published in the database maintained by the controller (Sec. 26).
- ❖ Duties of Certifying Authority (Secs. 30 – 34)
- ❖ To follow certain procedures regarding the security system (Sec. 30).
- ❖ The Act has laid down certain procedures relating to the security system to be followed by the certifying authority in the performance of its services. It must :
 - ❖ make use of hardware, software, and procedures that are secure from intrusion and misuse
 - ❖ provide a reasonable level of reliable services
 - ❖ adhere to security procedures to ensure the secrecy and privacy of electronic signatures
 - ❖ be the repository of all Electronic Signature Certificates
 - ❖ publish information regarding its practices, Electronic Signature Certificates and current status of such certificates
 - ❖ observe the specified standards.
- ❖ The above stated security procedures must ensure the achievement of 4 objectives of a security system : Confidentiality, accessibility of information, consistency of information and authorized use of resources.
- ❖ To ensure compliance of the Act (Sec. 31).
- ❖ The certifying authority must ensure that every person employed or engaged by it complies with the provisions of the Act, rules, regulations or order, made thereunder.
- ❖ To display its licence (Sec. 32).
- ❖ The certifying authority must display its licence at a conspicuous place in the premises in which it carries on its business.
- ❖ To surrender its licence (Sec. 33).
- ❖ The certifying authority must surrender its licence to the controller on its suspension or revocation.
- ❖ To make certain disclosures (Sec. 34).
- ❖ The certifying authority is required to make the following disclosures :
 - ❖ Disclosure of Electronic Signature Certificate
 - ❖ Disclosure of Certification Practice Statement (CPS) ;“Certificate Practice Statement”
 - ❖ means a statement issued by a certifying authority to specify the practices that the certifying authority employs in issuing electronic signature certificates [Sec. 2(1)(k)]
 - ❖ It also outlines the CA's policies, practices and procedures for verifying keys and suspension, revocation and renewal of electronic signature certificates.
 - ❖ Disclosure of notice of revocation and suspension of Certificates of Certifying Authority
 - ❖ Disclosure of facts materially and adversely affecting the reliability of electronic signature certificate
 - ❖ Disclosure of adverse effects to affected person [Sec. 34(2)]. The authority is bound to
 - ❖ disclose to affected person about any event which may materially and adversely affect the integrity of the computer system or the conditions under which electronic signature certificate was granted. The certifying authority is required to act in accordance with the procedure specified in its CPS to deal with such event or situation.

7. List of Offences and the Corresponding Penalties in IT Act 2000.

Section	Offence	Punishment	Availability and Cognizability 
65	Tampering with Computer Source Code	Imprisonment up to 3 years or fine up to Rs 2 lakhs	Offence is Bailable, Cognizable and triable by Court of JMFC.
66	Computer Related Offences	Imprisonment up to 3 years or fine up to Rs 5 lakhs	Offence is Bailable, Cognizable and
66-A	Sending offensive messages through Communication service, etc...	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable and triable by Court of JMFC
66-B	Dishonestly receiving stolen computer resource or communication device	Imprisonment up to 3 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-C	Identity Theft	Imprisonment of either description up to 3 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-D	Cheating by Personation by using computer resource	Imprisonment of either description up to 3 years and /or fine up to Rs. 1 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC

66-E	Violation of Privacy	Imprisonment up to 3 years and /or fine up to Rs. 2 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
66-F	Cyber Terrorism	Imprisonment extend to imprisonment for Life	Offence is Non-Bailable, Cognizable and triable by Court of Sessions
67	Publishing or transmitting obscene material in electronic form	On first Conviction, imprisonment up to 3 years and/or fine up to Rs. 5 lakh On Subsequent Conviction imprisonment up to 5 years and/or fine up to Rs. 10 lakh	Offence is Bailable, Cognizable and triable by Court of JMFC
67-A	Publishing or transmitting of material containing sexually explicit act, etc.... in electronic form	On first Conviction imprisonment up to 5 years and/or fine up to Rs. 10 lakh On Subsequent Conviction imprisonment up to 7 years and/or fine up to Rs. 10 lakh	Offence is Non-Bailable, Cognizable and triable by Court of JMFC
67-B	Publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form	On first Conviction imprisonment of either description up to 5 years and/or fine up to Rs. 10 lakh On Subsequent Conviction imprisonment of either description up to 7 years and/or fine up to Rs. 10 lakh	Offence is Non-Bailable, Cognizable and triable by Court of JMFC

68	Failure to comply with the directions given by Controller	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.
69	Failure to assist the agency referred to in sub section (3) in regard interception or monitoring or decryption of any information through any computer resource	Imprisonment up to 7 years and fine	Offence is Non-Bailable, Cognizable.
69-A	Failure of the intermediary to comply with the direction issued for blocking for public access of any information through any computer resource	Imprisonment up to 7 years and fine	Offence is Non-Bailable, Cognizable.
69-B	Intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) in regard monitor and collect traffic data or information through any computer resource for cybersecurity	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable.
70	Any person who secures access or attempts to secure access to the protected system in contravention of provision of Sec. 70	Imprisonment of either description up to 10 years and fine	Offence is Non-Bailable, Cognizable.
70-B	Indian Computer Emergency Response Team to serve as national agency for incident response. Any service provider, intermediaries, data centres, etc., who fails to prove the information called for or comply with the direction issued by the ICERT.	Imprisonment up to 1 year and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable

71	Misrepresentation to the Controller to the Certifying Authority	Imprisonment up to 2 years and/ or fine up to Rs. 1 lakh.	Offence is Bailable, Non-Cognizable.
72	Breach of Confidentiality and privacy	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh.	Offence is Bailable, Non-Cognizable.
72-A	Disclosure of information in breach of lawful contract	Imprisonment up to 3 years and/or fine up to Rs. 5 lakh.	Offence is Cognizable, Bailable
73	Publishing electronic Signature Certificate false in certain particulars	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.
74	Publication for fraudulent purpose	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.

8. Explain the Indian Evidence Act of 1872.

The Indian Evidence Act,[1] originally passed in India by the Imperial Legislative Council in 1872, during the British Raj, contains a set of rules and allied issues governing admissibility of evidence in the Indian courts of law.

Importance

The enactment and adoption of the Indian Evidence Act was a path-breaking judicial measure introduced in India, which changed the entire system of concepts pertaining to admissibility of evidences in the Indian courts of law. Until then, the rules of evidences were based on the traditional legal systems of different social groups and communities of India and were different for different people depending on caste, community, faith and social position. The Indian Evidence Act introduced a standard set of law applicable to all Indians.

The law is mainly based upon the firm work by Sir James Fitzjames Stephen, who could be called the founding father of this comprehensive piece of legislation.

The Act

The Indian Evidence Act, identified as Act no. 1 of 1872,[2] and called the Indian Evidence Act, 1872, has eleven chapters and 167 sections, and came into force 1 September 1872. At that time, India was a part of the British Empire. Over a period of more than 125 years since its enactment, the Indian Evidence Act has basically retained its original form except certain amendments from time to time.

Amendments:

The Criminal Law Amendment Act, 2005

Applicability

When India gained independence on 15 August 1947, the Act continued to be in force throughout the Republic of India and Pakistan, except the state of Jammu and Kashmir.,[3] Since the independence of Bangladesh in 26th March 1971, it is in use throughout Bangladesh though some necessary amendments have been made. After 1947, the Act continues in force in India, but it was repealed in Pakistan in 1984 by the Evidence Order 1984 (also known as the "Qanun-e-Shahadat"). It also applies to all judicial proceedings in the court, including the court martial. However, it does not apply on affidavits and arbitration.

Contents

This Act is divided into three parts and there are 11 chapters in total under this Act.[2]

Part 1

Part 1 deals with relevancy of the facts. There are two chapters under this part: the first chapter is a preliminary chapter which introduces to the Evidence Act and the second chapter specifically deals with the relevancy of the facts.

Part 2

Part 2 consists of chapters from 3 to 6. Chapter 3 deals with facts which need not be proved,[4] chapter 4 deals with oral

evidence,[5] chapter 5 deals with documentary evidence and chapter 6 deals with circumstances when documentary evidence has been given preference over the oral evidence.[6]

Part 3

The last part, that is part 3, consists of chapter 7 to chapter 11. Chapter 7 talks about the burden of proof. Chapter 8 talks about estoppel, chapter 9 talks about witnesses, chapter 10 talks about examination of witnesses, and last chapter which is chapter 11 talks about improper admission and rejection of evidence.[7]

Indian Evidence Act Classic Classification

In the Evidence Act All the Provisions can be divided into two Categories

Taking the Evidence (By Court)

Parties to a proceeding before a court of law can adduce only admissible evidence. Admissible evidence are either "Fact in issue" or "Relevant Facts"[8] which are not excluded from being adduced by any other provisions of Indian Evidence Act, 1872. Section 3 of the Act defined Fact, Fact in issue and Relevant Facts.

According to section 59 and 60, facts can be proved by two ways, One is Orally and Second is Documentary (includes Electronic Documents), Oral Evidence mostly suggest the Verbal deposition before the Court (and not other wise), and Which includes oral statement regarding materials too, Documentary Evidence suggest the Documents. So The Evidence Regarding Matter which have number of Facts, for which Evidence by way of oral or Documentary produced before the court for its Evaluation for either one fact or facts. Court by going through those Documentary Evidence and Oral Evidence decide that particular fact and all facts are proved or not, or whether the fact or facts can be presumed to be proved?

Evaluation

In Evaluation as above said by looking into the Oral and Documentary Evidence Court decide whether particular fact is proved or not, or facts are proved or not, In Evaluation there are two concepts to prove facts; One is Prove (Prove, Disprove or Not prove) and Other is Presumption[9] (that fact is proved) (may Presume, Shall presume and Conclusive proof) After going to Oral and Documentary Evidence Court see that whether any fact or facts are proved by looking to such evidence or not? If at all no evidence is given or enough evidence is given for the fact its said fact is 'Not proved'; The second Concept for evaluation is "Presumption" In Evidence many Section suggest these presumptions, Where there is said Facts 'may presume', Court is extremely free to believe it or not and may ask to prove the fact, According to section 4 in 'shall presume' court has no discretion and should consider the fact as proved unless it is disproved, Where in any provision it is said that particular fact, or particular fact in particular circumstances must be concluded as "conclusive proof" Court has to regard it as proved and shall not allow parties to adduce evidence to rebut it.[10]

Classification of Evidence Act in Four Questions

Evidence Act may be divided in four questions. Question 1 What is the Evidence given of? Answer 1 of Facts ("Issue of Facts" or "Relevant Facts") Question 2 How the Evidence of such Facts are Given Answer 2 The Evidence of Such Facts is Given Either by way of "Oral Evidence" or "Documentary Evidence" Question 3 On whom does the Burden of proof lie? Answer 3 "Burden of Proof"(of particular fact) or "Onus of proof" (to prove whole case) lies on the Prosecution incharge Question 4 What are the Evaluation of the Facts. Answer

4 The Evaluation is "Prove" or "Presumption"(of prove); The fact is either 'proved','disproved', or 'Not proved'; or there may be presumption that proof of facts "may presume', 'shall presume', or 'conclusive proof'.

9. Explain Bankers' Books Evidence Act 1891.

Bankers' Books Evidence Act, 1891 is an act in India dating from the British colonial rule, that is still in force largely unchanged.

History

In the late 19th century, the banking industry in India was a rapidly developing industry. Every year, new banks were being established, some by Indian businessmen, and others by mostly European owners. The main question which arose was whether the rules of evidence in Indian banking would be governed by British legislation, as India was then a British colony.

As a result it was decide to adapt and adopt the Bankers' Books Evidence Act, 1879 of the British Parliament to Indian banking. The Indian Bankers' Books Evidence Act, 1891 was therefore enacted and continues to be in force to the present day.

Tenets and Precepts[edit]

The main tenets and precepts of the Act are that whenever any Bank or Banker is compelled to provide evidence to a court or judge, the original documents need not be produced and that a copy of the original documents are sufficient for legal purposes.

Today, the Act is also in force in the former British colonies of Pakistan and Bangladesh, which were formerly ruled as parts of undivided India.

Review and Reform

The Act has been further amended by the Information Technology Act, 2000 which expanded the meaning and scope of Bankers Books to include computer documents, files and external storage. Now any banking related evidence can be produced in electronic format with no requirement for paperwork.

10. Explain Reserve bank of India Act, 1934.

Reserve Bank of India Act, 1934 is the legislative act under which the Reserve Bank of India was formed. This act along with the Companies Act, which was amended in 1936, were meant to provide a framework for the supervision of banking firms in India.

Summary

The Act contains the definition of the so-called scheduled banks, as they are mentioned in the 2nd Schedule of the Act. These are banks which were to have paid up capital and reserves above 5 lakh.

There are various section in the RBI Act but the most controversial and confusing section is Section 7. Although this section has been used only once by the central govt, it puts a restriction on the autonomy of the RBI. Section 7 states that central government can legislate the functioning of the RBI through the RBI board, and the RBI is not an autonomous body.

Section 17 of the Act defines the manner in which the RBI (the central bank of India) can conduct business. The RBI can accept deposits from the central and state governments without interest. It can purchase and discount bills of exchange from commercial banks. It can purchase foreign exchange from banks and sell it to them. It can provide loans to banks and state financial corporations. It can provide advances to the central government and state governments. It can buy or sell government securities. It can deal in derivative, repo and reverse repo.

Section 18 deals with emergency loans to banks. Section 21 states that the RBI must conduct banking affairs for the central government and manage public debt. Section 22 states that only the RBI has the exclusive rights to issue currency notes in India. Section 24 states that the maximum denomination a note can be is ₹10,000 (US\$140).

Section 26 of Act describes the legal tender character of Indian bank notes.

Section 28 allows the RBI to form rules regarding the exchange of damaged and imperfect notes.

Section 31 states that in India, only the RBI or the central government can issue and accept promissory notes that are payable on demand. However, cheques, that are payable on demand, can be issued by anyone.

Section 42(1) says that every scheduled bank must have an average daily balance with the RBI. The amount of the deposit shall be more than a certain percentage of its net time and demand liabilities in India.

11. What is Cyber Appellate Tribunal? What are its power?

The Information Technology Act, 2000 also provides for the establishment of the Cyber Appellate Tribunal. In this article, we will look at the establishment, composition, jurisdiction, powers, and procedures of a Cyber Appellate Tribunal.

Establishment of Cyber Appellate Tribunal (Section 48)

The Central Government notifies and establishes appellate tribunals called Cyber Regulations Appellate Tribunal.

The Central Government also specifies in the notification all the matters and places which fall under the jurisdiction of the Tribunal.

The composition of Cyber Appellate Tribunal (Section 49)

The Central Government appoints only one person in a Tribunal – the Presiding Officer of the Cyber Appellate Tribunal.

The qualifications for appointment as Presiding Officer of the Cyber Appellate Tribunal (Section 50)

A person is considered qualified for the appointment as the Presiding Officer of a Tribunal if – He has the qualification of the Judge of a High Court

He is or was the member of the Indian Legal Service and holds or has held a post in Grade I of that service for at least three years.

Procedure and powers of the Cyber Appellate Tribunal (Section 58)

The Code of Civil Procedure, 1908 does not bind the Cyber Appellate Tribunal. However, the principles of natural justice guide it and it is subject to other provisions of the Act. The Tribunal has powers to regulate its own procedure.

In order to discharge its functions efficiently, the Tribunal has the same powers as vested in a Civil Court under the Code of Civil Procedure, 1908, while trying a suit in the following matters:

Summoning and enforcing the attendance of any person and examining him under oath

Ensuring the availability of the required documents or electronic records

Receiving evidence on affidavits

Issuing commissions for examining witnesses or documents

Reviewing its decisions

Dismissing an application for default or deciding it ex-parte, etc.

Every proceeding before the Cyber Appellate Tribunal is like a judicial proceeding within the meaning of sections 193 and 228 and for the purposes of section 196 of the Indian Penal Code. Further, the Tribunal is like a Civil Court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.

12. What are the objectives of IT Act 2000?

The primary objectives of the IT Act, 2000 are:

Granting legal recognition to all transactions done through electronic data exchange, other means of electronic communication or e-commerce in place of the earlier paper-based communication.

Providing legal recognition to digital signatures for the authentication of any information or matters requiring

authentication.

Facilitating the electronic filing of documents with different Government departments and also agencies.

Facilitating the electronic storage of data

Providing legal sanction and also facilitating the electronic transfer of funds between banks and financial institutions.

Granting legal recognition to bankers for keeping the books of accounts in an electronic form. Further, this is granted under the Evidence Act, 1891 and the Reserve Bank of India Act, 1934.

13. What does IT Act, 2000, "Penalties and Adjudication" cover? Explain.

43. [Penalty and compensation] for damage to computer, computer system, etc.

➤

If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network,

Accesses or secures access to such computer, computer system or computer network [or computer resource]

downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium

introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network

damages or causes to be damaged any computer, computer system or computer network, data,

computer database or any other programmes residing in such computer, computer system or computer network

disrupts or causes disruption of any computer, computer system or computer network

denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means

provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under

charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network

destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means

steal, conceal, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage

43A. [Compensation for failure to protect data]

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and there by causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

46. [Power to adjudicate]

For the purpose of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made there under which renders him liable to pay penalty or compensation, the Central Government shall, subject to the provisions of sub-section (3), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry in the manner prescribed by the Central Government.

A. The adjudicating officer appointed under sub-section (1) shall exercise jurisdiction to adjudicate matters in which the claim for injury or damage does not exceed rupees five crore: Provided that the jurisdiction in respect of the claim for injury or damage exceeding rupees five crores shall vest with the competent court.

The adjudicating officer shall, after giving the person referred to in sub-section (1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section.

No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and legal or judicial experience as maybe prescribed by the Central Government.

Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.

Every adjudicating officer shall have the powers of a civil court which are conferred on the — Appellate Tribunal under sub-section (2) of section 58

47. [Factors to be taken into account by the adjudicating officer]

While adjudging the quantum of compensation under this Chapter, the adjudicating officer shall have due regard to the following factors, namely:—

The amount of gain of unfair advantage, wherever quantifiable, made as a result of the default

The amount of loss caused to any person as a result of the default;

The repetitive nature of the default.

14. Explain IT Act. 2008 and its Amendments

The Information Technology Amendment Act, 2008 (IT Act 2008) is a substantial addition to India's Information Technology Act (ITA-2000). The IT Amendment Act was passed by the Indian Parliament in October 2008 and came into force a year later. The Act is administered by the Indian Computer Emergency Response Team (CERT-In).

The original Act was developed to promote the IT industry, regulate e-commerce, facilitate e-governance and prevent

cybercrime. The Act also sought to foster security practices within India that would serve the country in a global context. The Amendment was created to address issues that the original bill failed to cover and to accommodate further development of IT and related security concerns since the original law was passed.

Changes in the Amendment include: redefining terms such as "communication device" to reflect current use; validating electronic signatures and contracts; making the owner of a given IP address responsible for content accessed or distributed through it; and making corporations responsible for implementing effective data security practices and liable for breaches.

The Amendment has been criticized for decreasing the penalties for some cybercrimes and for lacking sufficient safeguards to protect the civil rights of individuals. Section 69, for example, authorizes the Indian government to intercept, monitor, decrypt and block data at its discretion. According to Pavan Duggal, a cyber law consultant and advocate at the Supreme Court of India, "The Act has provided Indian government with the power of surveillance, monitoring and blocking data traffic. The new powers under the amendment act tend to give Indian government a texture and color of being a surveillance state."