# Unit-4

## 1. Foreign Exchange Management Act, 1999

**Introduction:**

The Foreign Exchange Management Act (FEMA) was introduced by the Government of India in 1999. It replaced the previous Foreign Exchange Regulation Act (FERA) of 1973, which was ineffective due to the liberalisation practices of India's government. The new Act allowed for a new management system in line with the World Trade Organisation.

To facilitate the flow of payments and trade to foreign countries and promote the smooth development of the market for foreign exchange in India, the Government of India adopted the Foreign Exchange Management Act (FEMA) 1999.

The Government of India, Ministry of Finance, vide Notification No.GSR(371)(E) dated 1st May 2000 has notified that the Foreign Exchange Management Act, 1999 (42 of 1999) shall come into force on the 1st day of June 2000.

The FEMA also set the stage in the direction of the Prevention of Money Laundering Act 2002, which was passed at the end of July. The FEMA also allowed the Reserve Bank of India to establish regulations and guidelines about foreign exchanges, which conform with India's foreign trade policies.

**What is the FEMA Act?**

The central government developed the FEMA to promote cross-border trade and foreign exchange payments. It was first introduced in 1999 to replace FERA, and FEMA is useful to fix all loopholes and shortcomings of FERA. Thus, the FEMA Act(Foreign Exchange Management Act) added several big modifications.

The FEMA is an act of the government that consolidated and modified the laws governing India's foreign exchange market. This FEMA Act's objective was to promote external payments, orderly development and the maintenance of the markets for foreign exchange in India.

A foreign investor or an Indian investor invests outside of India. Also, the investor must meet India's Foreign Exchange Regulations. The Directorate of Foreign Trade and the RBI has formed

these regulations. These regulations introduced foreign exchange compliance to keep an eye on the increasing flow of outbound and inbound funds.

**The Characteristics and Objectives of FEMA**

- The FEMA Act does not permit foreign security transfers or foreign exchange dealings for the unauthorised.
- FEMA doesn't allow those who reside outside of India.
- Facilitating the exchange of foreign currency and accounts for payments to fulfil the FEMA Act's primary responsibility and modification and consolidation of laws on foreign exchange. The Indian government implemented this law to promote orderly development and maintain the foreign exchange market in India.
- The FEMA Act 1999 requires that any person living in India receive the proceeds of a Forex payment without an equivalent remittance inward from overseas. The person concerned will be deemed to have accepted the payment from an unauthorised source.
- Certain prescribed limits were increased following the introduction of the FEMA Act 1999.
- There are seven types of transactions forbidden in the current account. This includes transactions related to lotteries, banned magazines, football pools and others.
- Foreign exchange management act 1999's stringent rules greatly impacted international trade transactions. The Act enticed foreign exchange and different payment options. Regularly, RBI releases notifications and circulars describing the changes made to certain sections of the FEMA Act.
- A resident of India can have securities, shares and property he bought during his time as a resident or inherits these properties from the resident.
- FEMA gives you the freedom to own or transfer any security outside India.

**How is the Foreign Exchange Management Act Applied?**

The FEMA Act is available to the entirety of India, and the agencies and offices located outside of India are run as owned or operated by an Indian citizen. The FEMA's headquarters is in New Delhi, and we call it the Enforcement Directorate.

**In particular, the FEMA Act 1999 applies to:**

- Financial, banking and insurance services
- Exporting any product/service in India to some other country
- Indian foreign exchange
- Indian foreign security
- The purchase, exchange or sale of any nature
- Any company in the world owned by a Non-Resident Indian (NRI)
- Importing any product or service from outside India
- Securities as per the Public Debt Act of 1994
- Any person who is a citizen of India who lives or resides in India or a different country

**The Government of India has classified FEMA into two categories:**

- Current Account Transactions — all trade of merchandise as an indicator of an economy's status.
- Capital Account Transactions — all capital transactions and the inflow and outflow of money to and from India.

**Current Account Transactions**

It consists of the flow and outflow of funds from specific countries that are not part of India during the year. The transaction occurs due to trade or rendering commodities, services or income exchange between these countries. After that, such transactions are classified into three different parts by foreign exchange regulations.

They include:

- Transactions that FEMA does not permit.
- The transaction requires RBI's prior approval.
- The transaction requires prior permission from the central government.

**The Restrictions on Dealing with Foreign Exchange**

The restrictions on dealing with foreign exchange are outlined in section 3 of the Act. The section reads as follows:

1. An authorised person can deal with the transfer of any security or currency to anyone.

2. It isn't advisable to make any payments to or on behalf of any resident who is not from India.
3. Only an authorised person can accept any order payment for any other person living outside of India.

Furthermore, Section 4 of the Act stipulates that no Indian resident can acquire or be an owner, hold, transfer or possess foreign currency/security or any immovable property outside India.

**Current Account transactions listed by FEMA have been classified into three areas:**

- Transactions prohibited by FEMA Act
- A transaction that requires Central Government's permission
- A transaction that requires the Reserve Bank of India's (RBI's) permission

**What Prohibitions Are Made Under FEMA Act In India?**

- Sending money which is the result of winning the lottery.
- Sending money which is the result of winning horse racing, cricket games, etc.
- Sending money to buy a lottery ticket, football betting, sweepstakes, banned publications, etc.
- The payment of commission on exports towards equity investment of Indian companies in joint ventures or wholly-owned subsidiaries abroad.
- The sending of a dividend by any company. This is only applicable if dividend balancing is applicable.
- The payment of commission on exports under Rupees State Credit Routes (except commission up to 10 percent of the invoice value of export of tea and tobacco).
- Any payment regarding "Call-back Services" of telephones.
- Any travel to Bhutan and/or Nepal.
- Sending interest income on funds held in Non-resident Special Rupees (NRSR) scheme account.
- A transaction of any kind with a resident of Bhutan or Nepal.

**The following foreign transactions require the approval of the Central Government:**

- Cultural tours.
- Advertising in foreign print media for any purpose other than promoting tourism, investments exceeding US$10,000 by a State Government or its Public Sector Undertaking.
- Payment of importation by a Public Sector Undertaking on cost, insurance, and freight on ocean transport.
- Payment for chartered freight vessels.
- Payment of shipping container detention charges above the Director-General of Shipping's (DGS's) rate.
- Payment of prize money or sponsorship money for any activity. Payment of any sport participated outside of India (other than national/international level sports) if it exceeds US$1,00,000.
- The payment for hiring transponders for internet service providers or television channels.
- Payment of Protection and Indemnity (P&I) Club membership.
- Payment for multi-model transport operators and their agencies abroad.

**What Are The Rules Of Trade For Foreign Exchange Management Act (FEMA) In India?**

According to the RBI, foreign exchange can be undertaken with any authorized dealer via the Prior Approval Route or General Permission Route.

| Scenario | Limitations |
|---|---|
| **Visiting privately to any country (except Bhutan and Nepal)** | Liberalized Remittance Scheme (LRS) limit of USD 2,50,000/- per year. |
| **Personal donations/gifts by resident individuals** | Liberalized Remittance Scheme (LRS) limit of USD 2,50,000/- per year. |
| **Corporate Donations by persons other than** | **One per cent** of the forex earnings |

| | |
|---|---|
| **resident individual** | during the preceding three financial years.<br>**OR**<br>**US$ 5,000,000,** whichever is less, for a specified purpose. |
| **Leaving India for the purposes of gainful employment** | Liberalized Remittance Scheme (LRS) limit of USD 2,50,000/- per year. |
| **Payment for emigration** | Liberalized Remittance Scheme (LRS) limit of USD 2,50,000/- per year. |
| **Payment for the care of relatives** (only close relatives) outside of India by a person who is resident but not permanently resident in India | The salary (after deducting income tax, Provident Fund, and other deductions) of a person not being a permanent resident in India and a citizen of a foreign state other than Pakistan.<br>OR<br>US$2,50,000/- a year per recipient in all other cases. |
| **Business travel abroad** | US$250,000 per year. |
| **Attending a training course or conference** | US$250,000 per year. |
| **For overseas medical treatment** | US$250,000 per year. |
| **The care of a patient going for a medical check-up or medical treatment abroad.** | US$250,000 per year. |
| **The care of a patient going for a medical check-up** | US$250,000 per year. |

| | |
|---|---|
| **or medical treatment abroad.** | |
| **Studying abroad** | US$250,000 per academic year or the education institution's estimation, whichever is higher |
| **Meeting the expenses of a person accompanying a patient going for a medical check-up or for medical treatment abroad** | US$250,000 per year. |
| **Commission payment to an agent outside India for selling of commercial or residential land or property in India** | US$25,000 or five percent of the transaction, whichever is higher. |
| **Consultancy services from overseas** | US$10,000,000 per project (for infrastructure projects). **For all other projects, US$1,000,000 per project** |
| **Pre-incorporation expense reimbursements** | US$100,000 or five percent of the investment brought into India, whichever is higher. |

**What Are the Transactions of the Capital Account?**

The capital account identifies any domestic investments inside the foreign assets, and a capital account checks foreign assets with domestic investments and vice versa. The FEMA Act states that the transactions of capital accounts change the liabilities/assets of an individual who lives inside or outside of India or liabilities/assets in India of the individual living outside India.

**Where is FEMA act applicable in India?**

FEMA act applies to all of India and the agencies and offices located outside of India that are managed or owned by an Indian citizen. The headquarters of FEMA is situated in New Delhi and is known as the Enforcement Directorate.

**What Are the Penalties Under FEMA?**

Suppose a taxpayer has committed an offence under this law in their tax evasion. In that case, they will be liable to pay the penalty equivalent to thrice the amount resulting from this default if the amount is quantifiable or the sum of **₹2 lakhs** isn't quantifiable.

If the taxpayer continues to commit the offence, the penalty amount could be up to **₹5000** per day for every day that they are in non-payment. The authority in charge is authorised to seize the currency, security or additional property owned by the person being assessed. Additionally, the officer has the power to transfer the money earned by the defaulter in foreign exchange to India.

**Distinguish between FERA & FEMA?**

Difference between the Foreign Exchange Regulation Act (FERA) and Foreign Exchange Management Act (FEMA) is explained here in detail.

The major differences between FERA and FEMA are:

| Foreign Exchange Regulation Act (FERA) | Foreign Exchange Management Act (FEMA) |
|---|---|
| Parliament of India passed the Foreign Exchange Regulation Act in 1973 | Parliament of India enacted the Foreign Exchange Management Act (FEMA) on 29 December 1999 replacing FERA. |
| FERA came into force from January 1, 1974. | FEMA came into force from June 2000. |
| FERA was repealed in 1998 by Vajpayee Government | FEMA succeeded FERA |
| FERA has 81 sections | FEMA has 49 sections |
| FERA was conceived with the notion that Foreign Exchange is a scarce resource. | FEMA was conceived with the notion that Foreign Exchange is an asset. |
| FERA rules regulated foreign payments. | FEMA focused on increasing the foreign exchange reserves |

| | |
|---|---|
| | of India, focused on promoting foreign payments and foreign trade. |
| The objective of FERA was conservation of Foreign Exchange | The objective of FEMA is Management of Foreign Exchange |
| The definition of "Authorized Person" was narrow. | The definition of "Authorized Person" was widened |
| Banking units did not come under the definition of Authorized Person. | Banking units came under the definition of Authorized Person. |
| If there was a violation of FERA rules, then it was considered as Criminal offence. | If there was a violation of FEMA rules, then it is considered as civil offence |
| A person accused of FERA violation was not provided legal help. | A person accused of FEMA violation will be provided legal help. |
| There was no provision for Tribunal, the appeals were sent to High Courts | There is provision for Special Director (Appeals) and Special Tribunal |
| For those guilty of violating FERA rules, there was provision for direct punishment. | For those guilty of violating FEMA rules, they have to pay a fine, starting from the date of conviction, if the penalty is not paid within 90 days, then the guilty will be imprisoned. |
| If there was a need for transferring of funds for external operations, then prior approval of the Reserve Bank of India (RBI) is required. | For External trade and remittances, there is no need for prior approval from the Reserve Bank of India (RBI). |
| There was no provision for IT | There is provision for IT |

# 2. Cyber Law

**Introduction**

"Cyber" is a prefix used to describe a person, thing, or idea as part of the computer and information age. Taken from *kybernetes*, Greek word for "steersman" or "governor," it was first used in cybernetics, a word coined by Norbert Wiener and his colleagues. The virtual world of internet is known as cyberspace and the laws governing this area are known as Cyber laws and all the netizens of this space come under the ambit of these laws as it carries a kind of universal jurisdiction. Cyber law can also be described as that branch of law that deals with legal issues related to use of inter-networked information technology. In short, cyber law is the law governing computers and the internet.

The growth of Electronic Commerce has propelled the need for vibrant and effective regulatory mechanisms which would further strengthen the legal infrastructure, so crucial to the success of Electronic Commerce. All these regulatory mechanisms and legal infrastructures come within the domain of Cyber law. Cyber law is important because it touches almost all aspects of transactions and activities on and involving the internet, World Wide Web and cyberspace. Every action and reaction in cyberspace has some legal and cyber legal perspectives. Cyber law encompasses laws relating to –

- Cyber crimes
- Electronic and digital signatures
- Intellectual property
- Data protection and privacy

Cyber Law also called IT Law is the law regarding Information-technology including computers and the internet. It is related to legal informatics and supervises the digital circulation of information, software, information security, and e-commerce.

IT law does not consist of a separate area of law rather it encloses aspects of contract, intellectual property, privacy, and data protection laws. Intellectual property is a key element of IT law. The area of software license is controversial and still evolving in Europe and elsewhere.

**According to the Ministry of Electronics and Information Technology, Government of India:**

*Cyber Laws yields legal recognition to electronic documents and a structure to support e-filing and e-commerce transactions and also provides a legal structure to reduce, check cyber crimes.*

## Role / Importance of Cyber Law:

1. It covers all transactions over the internet.
2. It keeps eye on all activities over the internet.
3. It touches every action and every reaction in cyberspace.

**Area of Cyber Law:**

Cyber laws contain different types of purposes. Some laws create rules for how individuals and companies may use computers and the internet while some laws protect people from becoming the victims of crime through unscrupulous activities on the internet. The major areas of cyber law include:

1. ***Fraud*:**

   Consumers depend on cyber laws to protect them from online fraud. Laws are made to prevent identity theft, credit card theft, and other financial crimes that happen online. A person who commits identity theft may face confederate or state criminal charges. They might also encounter a civil action brought by a victim. Cyber lawyers work to both defend and prosecute against allegations of fraud using the internet.

2. ***Copyright*:**

   The internet has made copyright violations easier. In the early days of online communication, copyright violations were too easy. Both companies and individuals need lawyers to bring an action to impose copyright protections. Copyright violation is an area of cyber law that protects the rights of individuals and companies to profit from their

creative works.

3. ***Defamation*:**

Several personnel uses the internet to speak their mind. When people use the internet to say things that are not true, it can cross the line into defamation. Defamation laws are civil laws that save individuals from fake public statements that can harm a business or someone's reputation. When people use the internet to make statements that violate civil laws, that is called Defamation law.

4. ***Harassment and Stalking*:**

Sometimes online statements can violate criminal laws that forbid harassment and stalking. When a person makes threatening statements again and again about someone else online, there is a violation of both civil and criminal laws. Cyber lawyers both prosecute and defend people when stalking occurs using the internet and other forms of electronic communication.

5. ***Freedom of Speech*:**

Freedom of speech is an important area of cyber law. Even though cyber laws forbid certain behaviors online, freedom of speech laws also allows people to speak their minds. Cyber lawyers must advise their clients on the limits of free speech including laws that prohibit obscenity. Cyber lawyers may also defend their clients when there is a debate about whether their actions consist of permissible free speech.

6. ***Trade Secrets*:**

Companies doing business online often depend on cyber laws to protect their trade secrets. For example, Google and other online search engines spend lots of time developing the algorithms that produce search results. They also spend a great deal of time developing other features like maps, intelligent assistance, and flight search services to name a few. Cyber laws help these companies to take legal action as necessary to protect their trade

secrets.

7. ***Contracts and Employment Law*:**

Every time you click a button that says you agree to the terms and conditions of using a website, you have used cyber law. There are terms and conditions for every website that are somehow related to privacy concerns.

**Need for Cyber law**

In today's techno-savvy environment, the world is becoming more and more digitally sophisticated and so are the crimes. Internet was initially developed as a research and information sharing tool and was in an unregulated manner. As the time passed by it became more transactional with e-business, e-commerce, e-governance and e-procurement etc. All legal issues related to internet crime are dealt with through cyber laws. As the number of internet users is on the rise, the need for cyber laws and their application has also gathered great momentum.

In today's highly digitalized world, almost everyone is affected by cyber law. For example:

- Almost all transactions in shares are in demat form.
- Almost all companies extensively depend upon their computer networks and keep their valuable data in electronic form.
- Government forms including income tax returns, company law forms etc. are now filled in electronic form.
- Consumers are increasingly using credit cards for shopping.
- Most people are using email, cell phones and SMS messages for communication.
- Even in "non-cyber crime" cases, important evidence is found in computers / cell phones e.g. in cases of divorce, murder, kidnapping, tax evasion, organized crime, terrorist operations, counterfeit currency etc.

- Cyber crime cases such as 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, pornography etc are becoming common.

- Digital signatures and e-contracts are fast replacing conventional methods of transacting business.

Technology per se is never a disputed issue but for whom and at what cost has been the issue in the ambit of governance. The cyber revolution holds the promise of quickly reaching the masses as opposed to the earlier technologies, which had a trickledown effect. Such a promise and potential can only be realized with an appropriate legal regime based on a given socio-economic matrix.

**Important terms related to cyber law:**

- "Access" with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network. (Sec.2(1)(a) of IT Act, 2000)

- "Addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary. (Sec.2(1)(b) of IT Act, 2000)

- "Affixing Electronic Signature" with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of Electronic Signature. (Sec.2(1)(d) of IT Act, 2000)

- "Asymmetric Crypto System" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature. (Sec.2(1)(f) of IT Act, 2000)

- "Certifying Authority" means a person who has been granted a license to issue a Electronic Signature Certificate under section 24. (Sec.2(1)(g) of IT Act, 2000)

- "Communication Device" means Cell Phones, Personal Digital Assistance (Sic), or combination of both or any other device used to communicate, send or transmit any text, video, audio, or image. (Sec.2(1)(ha) of IT Act, 2000)
- "Computer" means 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 (Sec.2(1)(i) of IT Act, 2000)
- "Computer Network" means the interconnection of one or more Computers or Computer systems or Communication device through-
    - the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and
    - terminals or a complex consisting of two or more interconnected computers or communication device whether or not the interconnection is continuously maintained. (Sec.2(1)(j) of IT Act, 2000)
- "Computer Resource" means computer, communication device, computer system, computer network, data, computer database or software. (Sec.2(1)(k) of IT Act, 2000)
- "Computer System" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data, and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions. (Sec.2(1)(l) of IT Act, 2000)
- "Cyber cafe" means any facility from where access to the Internet is offered by any person in the ordinary course of business to the members of the public. (Sec.2(1)(na) of IT Act, 2000)

- "Cyber Security" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction. (Sec.2(1)(nb) of IT Act, 2000)

- "Data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer. (Sec.2(1)(o) of IT Act, 2000)

- "Digital Signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3. (Sec.2(1)(p) of IT Act, 2000)

- "Electronic Form" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device. (Sec.2(1)(r) of IT Act, 2000)

- "Electronic Record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche. (Sec.2(1)(t) of IT Act, 2000)

- "Electronic signature" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature. (Sec.2(1)(ta) of IT Act, 2000)

- "Function", in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer. (Sec.2(1)(u) of IT Act, 2000)

- "Information" includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche. (Sec.2(1)(v) of IT Act, 2000)
- "Intermediary" with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes. (Sec.2(1)(w) of IT Act, 2000)
- "Key Pair", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key. (Sec.2(1)(x) of IT Act, 2000)
- "Originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary. (Sec.2(1)(za) of IT Act, 2000)
- "Private Key" means the key of a key pair used to create a digital signature. (Sec.2(1)(zc) of IT Act, 2000)
- "Public Key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate. (Sec.2(1)(zd) of IT Act, 2000)
- "Secure System" means computer hardware, software, and procedure that -:

(a) are reasonably secure from unauthorized access and misuse;

(b) provide a reasonable level of reliability and correct operation;

(c) are reasonably suited to performing the intended functions; and

(d) adhere to generally accepted security procedures. (Sec.2(1)(ze) of IT Act, 2000) "Subscriber" means a person in whose name the Electronic Signature Certificate is issued. (Sec.2(1)(zg) of IT Act, 2000)

**Types of Cyber Crimes**

**1. Child Pornography**

It is one of the most serious offences. Abusers utilise the Internet to reach out to and sexually abuse youngsters all around the world. The proliferation of the internet has made children a tempting target for cybercriminals. Paedophiles use their phoney identities to lure children into their traps, including contacting them in chat rooms where they befriend them and steal personal information from their helpless victims. These paedophiles lure children onto the internet in order to sexually attack them or exploit them as a sex object.

**2. Hacking**

Hacking requires unauthorized device access and the modification of the device so as to enable continued access, as well as a change of the target machine set-up, purpose, or service, without awareness or consent of the system owners.

**3. Denial of service attack**

A denial-of-service assault is a very primitive technology that overwhelms the target computer's power, which contributes to server denial of access to other machines. There are numerous methods used by hackers to download a server.

**4. Virus dissemination**

This illegal activity type requires either direct or non-authorized entry to the operating system

by installing new applications that are classified as ss bugs, worms, or logic bombs. The unauthorized removal or deletion of machine data or the Internet function, which prohibits regular device functions, is obviously an illegal offence and is generally referred to as computer sabotage.

**5. Computer forgery**

This occurs as data is changed and processed in computerized records. However, machines may also be used as means to conduct forgery. The availability of computerized colour laser copies created a new wave of dishonest modification or replication.

**6. Credit card fraud**

Modern companies easily exchange cash with computer machine stored cash, which causes computer theft. Credit card identification and personal and financial credit card details are often targeted for organized crime. Assets in data format also have a significantly higher value than historically economic assets which contribute to a potentially higher economic class.

**7. Phishing**

Modern companies easily exchange cash with computer machine stored cash, which causes computer theft. Credit card identification and personal and financial credit card details are often targeted for organized crime. Assets in data format also have a significantly higher value than historically economic assets which contribute to a potentially higher economic class.

**8. Spoofing**

Get one machine on a network to have a separate computer, typically a computer with unique access rights, such that the other machines are accessed throughout the network.

**9. Cyberstalking**

Cyberstalking is a modern way of cyber-crime in our culture where a person is being pursued or monitored online. A cyber-stalker does not physically track his victim; after his online interaction, he gathers details on stalks, harasses him and utilizes verbal threats to intimidate him. It is a violation of your anonymity online.

**10. Threatening**

The suspect sends abusive emails or contacts the survivor in chat rooms.

**11. Salami attack**

In such a fraud, the suspect performs subtle modifications in such a way the changes go unnoticed. Criminal deducts tiny sums as at 2.50 per month from all the bank's customer's accounts and deposits it into their account. In this situation, no account manager can approach the bank for too little, but fraudulent profits are massive.

**12. Email bombing**

Sending massive amounts of mail to a victim, which could be an individual, an organisation, or even mail servers, causing the system or network to fail.

**13. Data diddling**

Involves altering raw data just before a computer processes it and then changing it back after the processing is completed.

**14. Virus / worms attacks**

Viruses are programmes that attach themselves to a computer or a file, then spread to other files and computers on a network. They usually have an impact on a computer's data by modifying or removing it. Unlike viruses, worms do not require a host to attach to. They simply generate working clones of themselves and repeat the process until all of the accessible memory on a computer has been used.

**15. Logic bombs**

This crime depends upon a happening of a particular conditional event. The clearest example is the Chernobyl virus, which was dormant for most of the year and only became active on a specific date.

**16. Trojan attacks**

A Trojan is an unlawful programme that operates from within by pretending to be an approved software and therefore disguising its true intentions.

**17. Internet time thefts**

This is when an unauthorised person uses Internet hours that have been paid for by another person. Until the victim reported it, this type of cybercrime had never been heard of. This crime

is normally prosecuted under the Indian Penal Code and the Indian Telegraph Act, Indian Penal Code, 1860, No. 45, Acts of Parliament, 1860 (India), Indian Telegraph Act, 1885, No. 13, Acts of Parliament, 1885 (India).

**18. Cyber Stalking**

Although there is no commonly accepted definition of cyberstalking, it is generally characterised as a cybercriminal's repeated acts of harassing or threatening behaviour directed at a victim via the Internet. Stalking is defined as repeated acts of harassment directed at a victim, such as following them, making harassing phone calls, murdering the victim's pet, vandalising their property, and leaving written messages or objects.

**19. Cybersquatting**

Obtaining a domain name in order to collect payment from the owner of a trademark (including a business name, trade name, or brand name) is known as cybersquatting, and it can also include typo squatting (where one letter is different). A trademark owner can win a cybersquatting case by proving that the defendant registered a domain name containing the plaintiff's distinctive trademark in bad faith and with the purpose to profit.

**20. Cyber Defamation**

Cyber defamation is defined as any negative statement intended to harm a person's company or reputation. Libel or slander can be used to defame someone. When defamation is carried out via computers and/or the Internet, it is known as cyber defamation.

**21. Keystroke Logging**

It Is capturing and recording the keystrokes of a user. This kind of tool is used to extract passwords and encryption keys and thus override security measures.

**22. Data Driven Attack**

A type of attack that is disguised as harmless data and performed by a user's or other programme to launch an attack. A data-driven attack on a firewall is a worry because it could pass past the firewall in data form and initiate an attack against a system behind the firewall.

**23. DNS Spoofing**

A type of spoofing that takes use of the Domain Name Service, which allows networks to translate textual domain names to the IP numbers used to route data packets.

**24. Dumpster diving**

A form of human intelligence (HUMINT) in which cast-off articles and information are scavenged in an attempt to obtain advantageous data.

**25. Electromagnetic intrusion**

Intentional introduction of electromagnetic pulses into transmission pathways in any way with the goal of fooling or confusing operators.

**CYBER LAW IN INDIA**

cyber laws are contained in the Information Technology Act, 2000 ("IT Act") which came into force on October 17, 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government. The following Act, Rules and Regulations are covered 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

**Rules / Provisions notified under the Information Technology Act, 2000**

a) The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

b) The Information Technology (Electronic Service Delivery) Rules, 2011

c) The Information Technology (Intermediaries guidelines) Rules, 2011

d) The Information Technology (Guidelines for Cyber Cafe) Rules, 2011

e) The Cyber Appellate Tribunal (Salary, Allowances and other terms and conditions of service of Chairperson and Members) Rules, 2009

f) The Cyber Appellate Tribunal (Procedure for investigation of Misbehaviour or Incapacity of Chairperson and Members) Rules, 2009

g) The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public), 2009

h) The Information Technology (Procedure and Safeguards for interception, monitoring and decryption of information) Rules, 2009

i) The Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009

j) The Information Technology (Use of electronic records and digital signatures) Rules, 2004

k) The Information Technology (Security Procedure) Rules, 2004

l) The Information Technology (Other Standards) Rules, 2003

m) The Information Technology (Certifying Authority) Regulations, 2001

n) Information Technology (Certifying Authorities) Rules, 2000

**OVERVIEW OF THE INFORMATION TECHNOLOGY ACT, 2000**

The Information Technology Act was enacted with a view to give a fillip to the growth of electronic based transactions, to provide legal recognition for ecommerce and e-transactions, to facilitate e-governance, to prevent computer based crimes and ensure security practices and procedures in the context of widest possible use of information technology worldwide.

**Applicability of the Act**

The Act will apply to the whole of India unless otherwise mentioned. It applies also to any offence or contravention there under committed outside India by any person. The Act shall not apply to the following documents or transactions –

- A negotiable instrument as defined in Sec.13 of the Negotiable Instruments Act, 1881;
- A power of attorney as defined in Sec.1A of the Powers of Attorney Act, 1882;
- A trust as defined in Section 3 of the Indian Trusts Act, 1882;
- A Will as defined in Sec.2(h) of the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called;
- Any contract for the sale or conveyance of immovable property or any interest in such property.

**Important provisions of the Act**

**1) Digital signature and Electronic signature**

Digital Signatures provide a viable solution for creating legally enforceable electronic records, closing the gap in going fully paperless by completely eliminating the need to print documents

for signing. Digital signatures enable the replacement of slow and expensive paper-based approval processes with fast, low-cost, and fully digital ones. The purpose of a digital signature is the same as that of a handwritten signature. Instead of using pen and paper, a digital signature uses digital keys (public-key cryptography). Like the pen and paper method, a digital signature attaches the identity of the signer to the document and records a binding commitment to the document. However, unlike a handwritten signature, it is considered impossible to forge a digital signature the way a written signature might be. In addition, the digital signature assures that any changes made to the data that has been signed cannot go undetected.

Digital signatures are easily transportable, cannot be imitated by someone else and can be automatically time-stamped. A digital signature can be used with any kind of message, whether it is encrypted or plaintext. Thus Digital Signatures provide the following three features:-

- **Authentication** - Digital signatures are used to authenticate the source of messages. The ownership of a digital signature key is bound to a specific user and thus a valid signature shows that the message was sent by that user.
- **Integrity** - In many scenarios, the sender and receiver of a message need assurance that the message has not been altered during transmission. Digital Signatures provide this feature by using cryptographic message digest functions.

- **Non Repudiation** – Digital signatures ensure that the sender who has signed the information cannot at a later time deny having signed it.

A handwritten signature scanned and digitally attached with a document does not qualify as a Digital Signature. An ink signature can be easily replicated from one document to another by copying the image manually or electronically. Digital Signatures cryptographically bind an electronic identity to an electronic document and the digital signature cannot be copied to another document.

**Digital Signature under the IT Act, 2000**

Digital signature means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3.

Section 3 deals with the conditions subject to which an electronic record may be authenticated by means of affixing digital signature which is created in two definite steps.

First, the electronic record is converted into a message digest by using a mathematical function known as 'Hash function' which digitally freezes the electronic record thus ensuring the integrity of the content of the intended communication contained in the electronic record. Any tampering with the contents of the electronic record will immediately invalidate the digital signature.

Secondly, the identity of the person affixing the digital signature is authenticated through the use of a private key which attaches itself to the message digest and which can be verified by anybody who has the public key corresponding to such private key. This will enable anybody to verify whether the electronic record is retained intact or has been tampered with since it was so fixed with the digital signature. It will also enable a person who has a public key to identify the originator of the message.

'**Hash function'** means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "Hash Result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible to derive or reconstruct the original electronic record from the hash result produced by the algorithm; that two electronic records can produce the same hash result using the algorithm.

Digital signatures are a means to ensure validity of electronic transactions however who guarantees about the authenticity that such signatures are indeed valid or not false. In order that the keys be secure the parties must have a high degree of confidence in the public and private keys issued. Digital Signature is not like our handwritten signature. It is a jumble of letters and digits.

**Electronic Signature**

Electronic signature has also been dealt with under Section 3A of the IT Act, 2000. A subscriber can authenticate any electronic record by such electronic signature or electronic authentication technique which is considered reliable and may be specified in the Second Schedule. Any electronic signature or electronic authentication technique will be considered reliable if-

(a) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or , as the case may be, the authenticator and of no other person;

(b) the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;

(c) any alteration to the electronic signature made after affixing such signature is detectable;

(d) any alteration to the information made after its authentication by electronic signature is detectable; and

(e) it fulfills such other conditions which may be prescribed.

An electronic signature will be deemed to be a secure electronic signature if-

(i) the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and

(ii) the signature creation data was stored and affixed in such exclusive manner as may be prescribed. (Sec.15)

An Amendment to the IT Act in 2008 introduced the term electronic signatures. The implication of this Amendment is that it has helped to broaden the scope of the IT Act to include new techniques as and when technology becomes available for signing electronic records apart from Digital Signatures.

**2) E-Governance**

E-governance or Electronic Governance is dealt with under Sections 4 to 10A of the IT Act, 2000.

It provides for legal recognition of electronic records and Electronic signature and also provides for legal recognition of contracts formed through electronic means.

Filing of any form, application or other documents, creation, retention or preservation of records, issue or grant of any license or permit or receipt or payment in Government offices and its agencies may be done through the means of electronic form.

The Government may authorise any any service provider to set up, maintain and upgrade the computerized facilities and perform such other services as it may specify, by notification in the Official Gazette for efficient delivery of services to the public through electronic means. Service provider so authorized includes any individual, private agency, private company, partnership firm, sole proprietor form 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.

The following are some of the eGovernance applications already using the Digital Signatures:-

• MCA21 – a Mission Mode project under NeGP (National e-governance plan) which is one of the first few e-Governance projects under NeGP to successfully implement Digital Signatures in their project

• Income Tax e-filing • Indian Railway Catering and Tourism Corporation (IRCTC)

• Director General of Foreign Trade (DGFT)

• RBI Applications (SFMS : structured Financial Messaging System)

• National e-Governance Services Delivery Gateway (NSDG)

• eProcurement

• eOffice

• eDistrict applications of UP, Assam etc

**3) Attribution, Acknowledgement and Dispatch of Electronic Records**

Attribution of electronic records is dealt with under Sec.11 of the IT Act, 2000. An electronic record will be attributed to the originator - if it was sent by the originator himself; by a person who had the authority to act on behalf of the originator in respect of that electronic record; or by an information system programmed by or on behalf of the originator to operate automatically.

According to Section 12, the addressee may acknowledge the receipt of the electronic record either in a particular manner or form as desired by the originator and in the absence of such requirement, by communication of the acknowledgement to the addresses or by any conduct that would sufficiently constitute acknowledgement. Normally if the originator has stated that the electronic record will be binding only on receipt of the acknowledgement, then unless such acknowledgement is received, the record is not binding. However, if the acknowledgement is not received within the stipulated time period or in the absence of the time period, within a reasonable time, the originator may notify the addressee to send the acknowledgement, failing which the electronic record will be treated as never been sent.

Time and place of dispatch and receipt of electronic record is covered under Sec.13 of the IT Act, 2000. The dispatch of an electronic record occurs when it enters a computer resource outside the control of the originator. Unless otherwise agreed between the originator and the addressee, the time of receipt of an electronic record will be determined as follows, namely –

a) if the addressee has designated a computer resource for the purpose of receiving electronic records – i. receipt occurs at the time when the electronic record enters the designated computer resource; or

ii. if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee; b) if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.

An electronic record is generally deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

If the originator or the addressee has more than one place of business, the principal place of business will be the place of business. If the originator or the addressee does not have a place of business, his usual place of residence will be deemed to be the place of business. "Usual Place of Residence", in relation to a body corporate, means the place where it is registered.

**4) Certifying Authorities**

A Certifying Authority is a trusted body whose central responsibility is to issue, revoke, renew and provide directories of Digital Certificates. Certifying Authority means a person who has been granted a license to issue an Electronic Signature Certificate under section 24.

Provisions with regard to Certifying Authorities are covered under Chapter VI i.e. Sec.17 to Sec.34 of the IT Act, 2000. It contains detailed provisions relating to the appointment and powers of the Controller and Certifying Authorities.

**Controller of Certifying Authorities (CCA)**

The IT Act provides for the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities. The Certifying Authorities (CAs) issue digital signature certificates for electronic authentication of users.

The CCA certifies the public keys of CAs using its own private key, which enables users in the cyberspace to verify that a given certificate is issued by a licensed CA. For this purpose it operates, the Root Certifying Authority of India (RCAI). The CCA also maintains the National Repository of Digital Certificates (NRDC), which contains all the certificates issued by all the CAs in the country.

**The functions of the Controller are** –

(a) to exercise supervision over the activities of the Certifying Authorities;

(b) certify public keys of the Certifying Authorities;

(c) lay down the standards to be maintained by the Certifying Authorities;

(d) specify the qualifications and experience which employees of the Certifying Authorities should possess;

(e) specify the conditions subject to which the Certifying Authorities shall conduct their business;

(f) specify the content of written, printed or visual material and advertisements that may be distributed or used in respect of a Electronic Signature Certificate and the Public Key;

(g) specify the form and content of a Electronic Signature Certificate and the key;

(h) specify the form and manner in which accounts shall be maintained by the Certifying Authorities;

(i) specify the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;

(j) facilitate the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;

(k) specify the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;

(l) resolve any conflict of interests between the Certifying Authorities and the subscribers;

(m)lay down the duties of the Certifying Authorities;

(n) maintain a data-base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to the public.

Controller has the power to grant recognition to foreign certifying authorities with the previous approval of the Central Government, which will be subject to such conditions and restrictions imposed by regulations.

**Procedures to be followed by Certifying Authorities**

Every Certifying Authority should –

(a) make use of hardware, software, and procedures that are secure from intrusion and misuse:

(b) provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;

(c) adhere to security procedures to ensure that the secrecy and privacy of the Electronic Signature are assured;

(d) be the repository of all Electronic Signature Certificates issued under the IT Act;

(e) publish information regarding its practices, Electronic Signature Certificates and current status of such certificates; and

(f) observe such other standards as may be specified by regulations.

**5) Electronic Signature Certificates**

Provisions relating to Electronic/Digital signature certificates are covered in Chapter VII i.e. Secs.35 to 39 of the IT Act, 2000 and Rules 23 to 30 of the IT (Certifying Authorities) Rules, 2000 and IT (Certifying Authority) Regulations, 2001.

A Digital Signature Certificate is an electronic document which uses a digital signature to bind together a public key with an identity — information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to the individual. Digital certificates are the digital equivalent (i.e. electronic format) of physical or paper certificates. Examples of physical certificates are driver's licenses, passports or membership cards.

Digital Signature Certificates is issued by the Certifying Authority (CA). The CA is responsible for vetting all applications for Digital Signature Certificates, and once satisfied, generates a Digital Certificate by digitally signing the Public key of the individual along with other information using its own Private key.

**6) Penalties and Offences Section under IT Act, 2000**

| Section under IT Act, 2000 | Offence | Penalty |
|---|---|---|
| Sec.43 | Damage to computer, computer system, etc. | Compensation not exceeding one crore rupees to the person so affected |
| Sec.43A | Body corporate failure to protect data | Compensation not exceeding five crore rupees to the person so affected |
| Sec.44(a) | Failure to furnish document, return or report to the Controller or the Certifying Authority | Penalty not exceeding one lakh and fifty thousand rupees for each such failure |
| Sec.44(b) | Failure to file any return or furnish any information, books or other documents within the time specified | Penalty not exceeding five thousand rupees for every day during which such failure continues |
| Sec.44(c) | Failure to maintain books of account or records | Penalty not exceeding ten thousand rupees for every day during which the failure continues |
| Sec.45 | Where no penalty has been separately provided | Compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five |

| | | |
|---|---|---|
| | | thousand rupees |
| Sec.65 | Tampering with Computer source documents | Imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both |
| Sec.66 | Hacking with Computer systems, Data alteration etc. | Imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both |
| Sec.66A | Sending offensive messages through communication service etc. | Imprisonment for a term which may extend to three years and with fine |
| Sec.66B | Retains any stolen computer resource or communication device | Imprisonment for a term which may extend to three years or with fine which may extend to rupees one lakh or with both |
| Sec.66C | Fraudulent use of electronic signature | Imprisonment for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh |
| Sec.66D | Cheats by personating by using computer resource | Imprisonment for a term which may extend to three years and shall also be liable to fine which may extend to |

| | | |
|---|---|---|
| | | one lakh rupees |
| Sec.66E | Publishing obscene images | Imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both |
| Sec.66F | Cyber terrorism | Imprisonment which may extend to imprisonment for life |
| Sec.67 | Publishes or transmits unwanted material description for a term which may extend to five years and also with fine which may extend to ten lakh rupees | Imprisonment for a term which may extend to three years and with fine which may extend to five lakh rupees & in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees |
| Sec.67A | Publishes or transmits sexually explicit material | Imprisonment for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and |

| | | |
|---|---|---|
| | | also with fine which may extend to ten lakh rupees |
| Sec.67B | Abusing children online | Imprisonment for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees |
| Sec.67C | Preservation of information by intermediary | Imprisonment for a term which may extend to three years and shall also be liable to fine |
| Sec.70 | Un-authorised access to protected system | Imprisonment for a term which may extend to ten years and shall also be liable to fine |
| Sec.71 | Misrepresentation to the Controller or the Certifying Authority for obtaining license or Electronic Signature Certificate | Imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both. |
| Sec.72 | Breach of Confidentiality and Privacy | Imprisonment for a term which may extend to two |

| | | |
|---|---|---|
| | | years, or with fine which may extend to one lakh rupees, or with both |
| Sec.72A | Disclosure of information in breach of contract | Imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both |
| Sec.73 & 74 | Publishing false digital signature certificates | Imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both |

**Jurisdiction**

If a crime is committed on a computer or computer network in India by a person resident outside India, then can the offence be tried by the Courts in India?

According to Sec.1(2) of Information Technology Act, 2000, the Act extends to the whole of India and also applies to any offence or contravention committed outside India by any person. Further, Sec.75 of the IT Act, 2000 also mentions about the applicability of the Act for any offence or contravention committed outside India. According to this section, the Act will apply to an offence or contravention committed outside India by any person, if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

**Advantages of Cyber Law:**

- Organizations are now able to carry out e-commerce using the legal infrastructure provided by the Act.
- Digital signatures have been given legal validity and sanction in the Act.
- It has opened the doors for the entry of corporate companies for issuing Digital Signatures Certificates in the business of being Certifying Authorities.
- It allows Government to issue notifications on the web thus heralding e-governance.
- It gives authority to the companies or organizations to file any form, application, or any other document with any office, authority, body, or agency owned or controlled by the suitable Government in e-form using such e-form as may be prescribed by the suitable Government.
- The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions.
- Cyber Law provides both hardware and software security.