Date : 20 12 2023
Page : 1 LAW

chp - 1 :

Introduction to cyber laws and Technology

- Cyber laws –

(1) cyber law is the law that deals with crimes done with the help of modern technology that is mainly through computer.

(2) The parliament of India passed its first cyber law that is through the Information technology act 2000, which provides the legal infrastructure for E-commerce in India.

(3) This law helps with the various legal formalities that E-commerce Apps and sites have to face.

(4) Another reason for passing this law is to protect the security of India so that it does not get threatened by people who can easily access through confidential datas with the help of a computer or any other electronic device.

- (5) Cyber law is any law that applies to the Internet and Internet related technology. thus, cyber law is the Branch of law that deals with the Internet's relationship to technological and electronic elements including computer SW, HW and Information system

(6) cyber law prevents or reduce large scale damage from cyber criminal activities by protecting Information access, privacy, communications, intellectual property and freedom of speech related to the use of the Internet, website, cell phones etc.

Date :
Page :

◆ Network Security -

(1) Nlw security protects your Nlw and data from breaches, intrusions and other threats.

(2) This is a vast term that describes Hlw and slw solutions as well as processes or rules and configurations relating to nlw use, accessability and overall threat protection.

(3) Nlw security involves access control, virus and antivirus slw application security. Nlw analytics, types of Nlw related security firewall VPNs etc.

• Types of Nlw security protection -

(1) Firewall -
firewall control incoming and outcoming traffic on networks with predetermine security rules. It keeps out untriendly traffic and is a necessary part of daily computing. Nlw security relies ~~hatt~~ heavily on firewalls and especially next generation firewalls which focus on locking malware and application layer attacks.

(2) Access control -
It defines the people or groups that the device have accessed to nlw application system thereby denying unsactioned access.

3. Email Security – Email Security refers to any process, products and services designed to protect your e-mail account and e-mail contents safe from external threats, Most email service provide us have built-in email security features design to keep your account secure.
but these may not enough to stop cyber criminal from access your information.

4. Data loss prevention (DLP)
5. ~~Introduct~~ Intrusion prevention system (IPS) } elaborate
6. Sandboxing.

03/01/24

chp-2
Legal Framework and Regulations

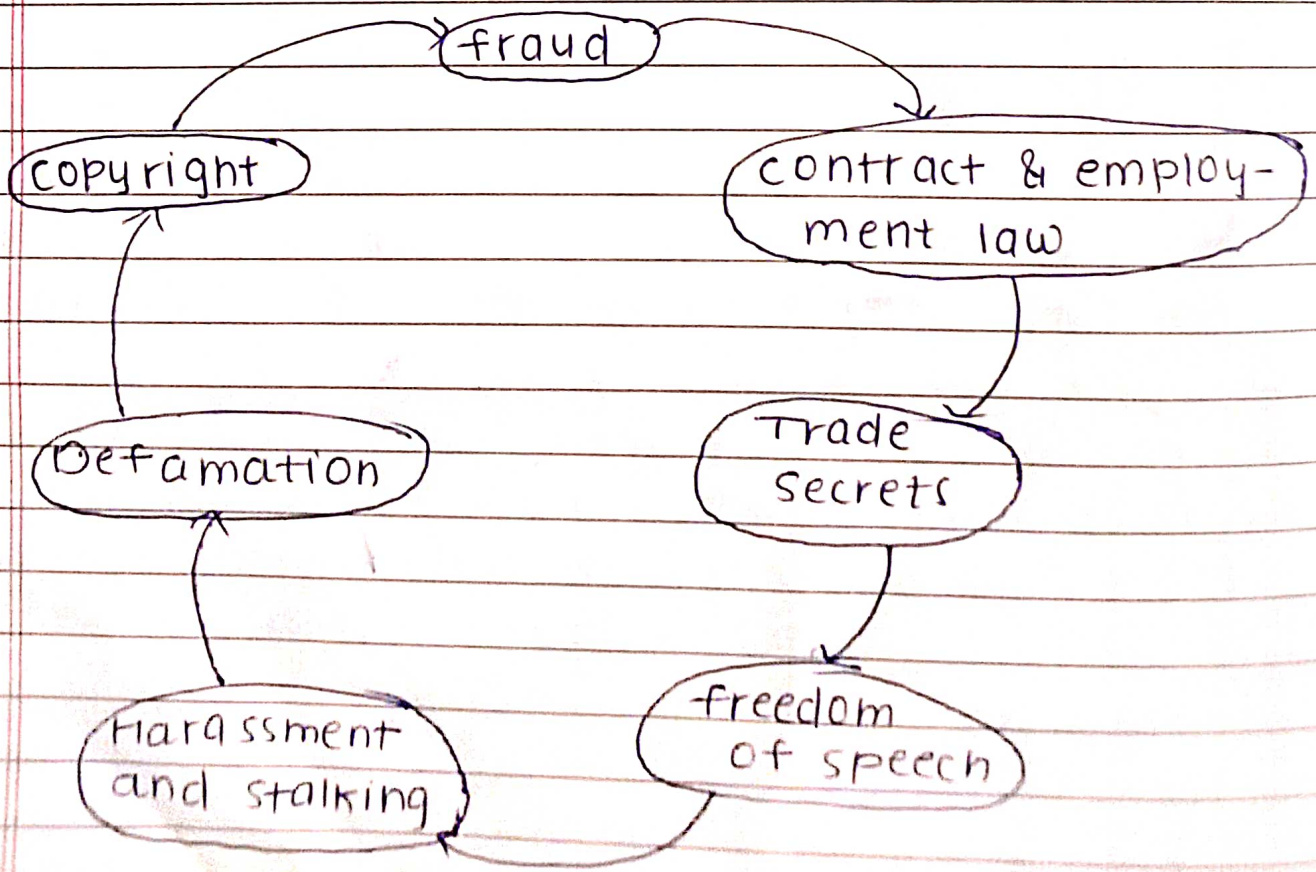
Date :
Page :

- Cyber law and Components of Cyber law

① The cyber law defination states that cyber security law comprises a number of directives that safe-guard information technology while facing organisation to protect their information and system from cyber attack using number of methods.

② On the other hand cyber crime laws are created for the offense and penalties for cyber crime. These law includes crimes that are directed at data, computers or information communication technologies and crimes comitted by people using ICT or computers.

- Component of cyber law



Date :
Page :

1. Fraud -

i. cyber laws are essential to consumers protection against fraud. legislation is created to stop online financial crime, including credit card theft, identify theft and others.

ii. cyber attorneys work to both defend and procecute client occured of online fraud.

2. copyrights -

i. copyright violations have become easier bcos of the internet.

ii. To file a lawsuit to impose copyright protecth businesses and individual both needs lawyers.

iii. cyber law defend people's and business's right to make money of their creative work in the domain of copyright violation.

3. Defamation -

i. Many employees use the internet to express themselves using the internet to spread untrue information might cross the line into defamation

ii. laws against defamations are civil laws that protect people from false public statement that might hurt someone's reputation or business.

iii. defamation legislation refers to when individuals use the internet to make claims that are illegal under civil laws.

iv. Their is a violation of both civil and criminal status when someone repetedly post threatening comments about another individual online.

Date :
Page :

4. Harassment and stalking -

i. criminal laws that prohibit stalking and harassment can occasionally be broken by online words.

ii. Their is a violation of both civil and criminal status when someone repetedly post threatening comments about another individual online.

iii. when stalking occurs online or through other electronic communication, cyber lawyers both prosecute and defend the victim.

04/01/24

Date :
Page :

5. Freedom of speech -

(i) Freedom of speech is an important area of cyber law even though cyber laws forbid certain behaviours online, freedom of speech laws also allows people to speak their minds.

(ii) cyber lawyers must advice their clients on the limits of the speech including laws. 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 there trade secrets. for example google and other online search engines spend lots of time developing the algorithm that produce search results. they also spend time on developing other features like maps, intelligent assistance etc.

cyber laws help these companies to take legal actions as necessary to protect their trade secrets.

7. Contracts and Employment Law –

Everytime you click a button that says you agree to the terms and conditions of using websites, you have used cyber law. there are terms and conditions for every websites that are somehow related to privacy concern.

- ~~Of~~ Advantages – Cyber Law :

(i) organizations are now able to carryout e-commerce using legal infrastructure provided by the act.

(ii) digital signature have been given legal validity and sanction in the act. it has opened the doors for the entry of corporate companies for issuing digital signature certificate in the business of being certifying authorities.

(iii) it allows government to issue notifications on the web thus making the use of e-governance.

(iv) IT act also addresses the important issues of security which are so critical to the success of electronic transactions.

(v) cyber law provide both HIW, SIW security

- Cyber law In India : An Overview of IT ACT : 2000

- History -

(i) the IT act : 2000 came into force on 17th october, 2000.

(ii) the act applies to whole of india and it's provisions also apply to any offence or contraventions, committed even outside the terroterial of republic of india.

(iii) In order to attract provisions of this act such as offence or contravention should involve in computer, computer system or computer n|w located in India.

(iv) the IT act : 2000 has tried to essimilate legal principles available in several such laws (relating to information technology) in-acted earlier in several countries. the act gives legal validity to electronic contracts, recognisition electronic signatures.

(v) This is a modern legislation which makes acts like hacking, data theft, spreading virus, deffemation, identity theft etc a criminal offence.

(vi) the act is supplemented by a no. of rules which includes rules for cyber cafes, electronic service delivery, data security and locking-off websites.

Date :
Page :

- Offences :

(1) section: 65 - Tempering with computer source document

(i) If a person knowingly or intentionally conceals, destroys or alters any computer source code used for a computer, computer programs, computer systems or computer N|w when the computer source code is required to be kept or maintained by law for the time being in force.

(ii) Penalty -
imprisonment upto 3 years and or with fine upto rupees 2 lac.

(2) section 66 - Hacking with computer systems

(i) if a person with the intend to cause or knowing that he is likely to cause wrongful ~~loss~~ loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it by any means, commits hack.

(ii) Penalty -
Imprisoment upto 3 years and or with fine upto rupees 5 lac.

(3) Section 66B – recieving stolen computer or communication device

(i) A person recieves or retains a computer resource or communication device which is known to be stolen or the person has reason to believed as stolen.

(ii) penalty –
imprisoment upto 3 years and or with fine upto rupees 1 lac.

(4) Section 66C – using password of another person

(i) A person fraudulently uses the password, digital signature or other unique identification of another person.

(ii) penalty –
imprisoment upto 3 years and or with fine upto rupees 1 lac.

(5) Section 66D – cheating using computer resource

(i) If a person cheats someone using a computer resource or communication

(ii) penalty –
imprisoment upto 3 years and or with fine upto rupees 1 lac

(6) Section 66E - Publishing private images of others

(i) If a person ~~captur~~ captures, transmit or publishes private images of other person without his/her concent or knowledge.

(ii) penalty -
Imprisoment upto 3 years and or with fine upto 2 lac.

10/01/24

(7) Section : 66F - Cyber Terrorism

(8) section 67 - Transmitting obsence material in electronic form.

penalty - imprisonment of ~~3~~ 5 years and or with fine upto 10 lac.

(9) section 67A - Transmission of any material containing sexually act through an electronic mode.

penalty - imprisonment of 7 years with fine 10 lac.

(10) Section 67B - depicting children in sexually explicit form and transmitting such materials through electronic mode.
penalty - imprisonment of 7 years and fine of 10 lac.

(11) section 67C - ~~failure~~ to preserve / retain the information by intermediaries
penalty - imprisonment of 3 years.

◆ objective of IT act : 2000

i) The act is to protect all transaction done through electronic
ii) Ecommerce reduce paper work used for communication purpose, it also leave to communicate and exchange of information through electronic

iii) It protect digital signature that are use for any short of legal ~~informati~~ authentication.
It regulate the activities of intermediaries by keeping or check on their powers.
iv) It defines various offences related to data privacy of citizens and enhance protect their data.
v) It also regulate and protect the sensitive data stored by social media and other electronic intermediation.

vi) It provides recognisition to book of account kept in electronic ~~from~~ form regulate by RBI (Reserve Bank of India) act 1934.

- Features -

- Amendments to IT ACT: 2000 -

1) with the advancement of time and technology it was necessary to bring some changes to the act to meet the need of society.

- Amendment of 2008

A) Section 66A : i) the amendment of 2008 would changes to section 66A of the act. this was the most controversiure as it provided the punishmnt for sending any offensive msg through electronic mode

ii) any msg or informath that created th or hampered the integrity or security of the country was prohibit However, it had not defined the word "offensive" what constitute such msgs. bcos which many of people arrested on this ground. this section further struct down by the supreme court in case of "shreya singhal" union of India.

B) Section 69A - Impowers the authority to intersept, monitor or decrypt any informath generated, transmitted, recieves or stored in any computer resource if it is necessary to do so in the interest of integrity of India, defence of India, the security of the state, friendly relation with foreign country or public order for preventing incitement offence of investigath of any offence. they also empower government to block I/H site in the interest of nation, the law also contain

ER - Electronic Record
DS - Digital signature.

procedural safeguard for blocking any site.
- when parties opposed to the sectn stated that this section violated the right to privacy the supreme Court contended that the national security is above individual privacy. - the apps code upheld the constitution validity of this sectn. the recent banning the chinese app was done siting provision under section 69A of the IT Act.

o Legal Recognition of Electronic Record & signature

a) recognition of electronic records - The IT act 2000 also aim to provide the legal framework under which legal security is accorded to all. ER and other activity carried out by electronic informath system controll & audit means. the act state that unless agreed on an expectance of contract may be expressed by electronic means of communicath and the same can have legal validity and enforceability.

b) Digital signature - section 3 : give legal recognith to ER and digital signature the DS is created in to distinct steps : 1) the ER converted into msg digest by using a hash function. which digitally frees. ER does ensuring the integrity of the ER. 2) The identify of person to a fixing the DS is authenticated through the use a private key which attaches itself. the msg digest and which can be verified by anybody who has the public key of private key.

c) Electronic signature - section 3A : an amendent the IT act 2008 introduce the terms ES.

ii) Implementath of the amendents is that help to broaden the scope of IT act to include new techniques as an when technology become available for signining Electronic record apart from Digital signature.

17/01/24

Date : 17 1 2024
Page :

- Cryptography -

i) It is a technique of securing information and communications through use of course so that only those person for whom the information is intended can understand it and process it. thus preventing unauthorised access to information.

ii) The prefix 'crypt' means 'hidden' and suffix 'graphy' means 'writing'.

iii) In cryptography the techniques which are used to protect information are obtained from mathematical concepts and a set of rules-based calculations known as algorithms.

iv) These algorithms are used for cryptographic key generation, digital signing, verification to protect data etc.

- Features of cryptography

1) Authentication
2) confidentiality
3) Integrity
4) Non-repudiation

} elaborate

- Applications -

Date :
Page :

o Encryption Techniques and algorithms -

i) Encryption is the method by which information is converted into secret codes that hides the information's true meaning.

ii) the science of encrypting and decrypting information is called cryptography.

iii) In computing un-encrypted data also know as plain text or clear text and encrypted data is also called as cipher text.

iv) The formulas used to encode and decode msgs are called encryption algorithms or ciphers.

v) To be effective a cipher includes a variable as a part of algorithm. variable which is used is called a key. and this key makes the ciphers output unique.

vi) when an encrypted msg is intercepted by an unauthorized entity, the intruder has to guess which ciphers the sender used to encrypt the msg. as well as what keys were used as variable..

vii) The time and difficulty of guessing this information is what makes encryption such as valuable security tools.

viii) encryption has been long standing way for sensentive information to be protected historically it was used by military and government

ix) in modern time it is used to protect data stored in computer and storage device as well as data which transmits over nlw.

ciphers - formula / algorithm

Date :
Page :

- How is encryption used?

i) encryption is commonly used to protect data so everytime someone uses ATM or buys something online with smartphone, encryption is used to protect the information.

ii) there are three major component to any encryption system -
a) the data
b) the encryption engine
c) key management

- How does encryption work?

i) First the sender must decide what cipher will best disguise the meaning of the message and what variable to use as a key to make the encoded message unique.

ii) Basically, there are two encryption techniques as symmetric & ciphers (formula / algorithm)

- they are also referred as secret key encryption which uses single or same key.
- the key is sometimes referred to as a shared secret because the key must be shared only with authorized entities.
- Symmetric key encryption is much faster than asymmetric key.

most widely used algorithm is AES algorithm.

b) Asymmetric ciphers -

also known as public key encryption used two different keys but logically linked key this type of cryptography often uses prime

18/01/24

Date :
Page :

numbers to create keys. since it is computationally to factor large prime numbers. most widely used algorithm is RSA algorithm.

- Digital signature and Electronic signature -

Both digital signature and electronic signature add authenticity and integrity to documents but in different ways.

▸ Electronic signature -

- when you digitally sign a document by typing your name in a designated signature field is an example of electronic signature.
- A scanned image of your handwritten signature that you insert into a document or a typed name at the end of an email can also be considered an electronic signature
- an electronic signature can be a image, file or a ~~simple~~ sympol attached to a document to give a consent for a signature.

▸ Electronic signature Types -

1) simple Electronic signature (SES) -
It is most basic type of electronic signature simple as typing your name, clicking a button that says "I agree". It doesn't require any special verification or proof of identity for signer.

II) Advance Electronic signature (AES) -
An AES is more sure then a simple electronic signature. this type of signature uses a digital certificate to verify the identity of the signer; ensuring that the signature is authentic and cannot be forged.

III) Qualified Electronic signature (QES) -
QES is most secure type of electronic signature It is created using a digital certificate issued by a qualified trust service provider (QTSP). QTSP is authorized by government to provide digital certificates and is responsible for verifying the identity of signer.

▶ Digital signature -
- It is a type of Electronic signature that uses cryptographic techniques to verify the authenticity and integrity of a digital document or message.
- It involves the use of public key infrastructure (PKI) which contains a pair of keys: a private key kept by the signer and a corresponding public key made available to others.
- the signer applies their private key to digitally sign the document, creating a unique digital finger print that can be verified using public key.
- the PKI provides a secure framework for verifying the identity of signer, preventing tampering with the document and enabling trust in business transaction.

ES - Electronic signature
DS - Digital signature.

Date :
Page :

o Differentiation between Electronic signature and Digital signature -

Digital signature are used to seal and identify a document to protect it from forgery. whereas ES are used to make sure that the terms within a document are treated as legally binding so long as the document has been marked with E-signature.

i) purpose -

biggest difference between DS and ES is that they are used to achieve different purposes. the main purpose of DS is to secure a document and verify that the document hasn't tampered or forged however an ES is used to indicate that a signer is actively and knowingly entering into a binding agreement or contract.

ii) common use cases -

ES are commonly used/added to business contracts to show that a signer chooses to agree with the terms laid out by the other party. on the other hand DS are often uced by certification authorities or trust service providers.
This bodies will validate DS and verify the digital document.