Unit-6

CYBER ETHICS AND LAWS

What is Cyber Law?

Cyber Law is the law governing cyber space. Cyber space is a very wide term and includes computers, networks, software, data storage devices. (Such as hard disks, USB disks etc.), the Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc. Law encompasses the rules of conduct: 1. That have been approved by the government, and 2. Which are in force over a certain territory, and 3. Which must be obeyed by all persons on that territory? Violation of these rules could lead to government action such as imprisonment or fine or an order to pay compensation. Cyber law encompasses laws relating to: 1. Cyber Crimes 2. Electronic and Digital Signatures 3. Intellectual Property 4. Data Protection and Privacy Cybercrimes are unlawful acts where the computer is used either as a tool or a target or both. The enormous growth in electronic commerce (e-commerce) and online share trading has led to a phenomenal spurt in incidents of cybercrime. Electronic signatures are used to authenticate electronic records. Digital signatures are one type of electronic signature. Digital signatures satisfy three major legal requirements – signer authentication, message authentication and message integrity. The technology and efficiency of digital signatures makes them more trustworthy than hand written signatures.

Intellectual property is refers to creations of the human mind e.g. a story, a song, a painting, a design etc. The facets of intellectual property that relate to cyber space are covered by cyber law. These include: Copyright law in relation to computer software, computer source code, websites, cell phone content etc. Software and source code licenses Trademark law with relation to domain names, Meta tags, mirroring, framing, linking etc. Semiconductor law which relates to the protection of semiconductor integrated circuits design and layouts, Patent law in relation to computer hardware and software. Data protection and privacy laws aim to achieve a fair balance between the privacy rights of the individual and the interests of data controllers such as banks, hospitals, email service providers etc. These laws seek to address the challenges to privacy caused by collecting, storing and transmitting data using new technologies.

Need for Cyber Law

There are various reasons why it is extremely difficult for conventional law to cope with cyberspace. Some of these are discussed below. 1. Cyberspace is an intangible dimension that is impossible to govern and regulate using conventional law. 2. Cyberspace has complete disrespect for jurisdictional boundaries. A person in India could break into a bank‖s electronic vault hosted on a computer in USA and transfer millions of Rupees to another bank in Switzerland, all within minutes. All he would need is a laptop computer and a cell phone. 3. Cyberspace handles gigantic traffic volumes every second. Billions of emails are crisscrossing the globe even as we read this, millions of websites are being accessed every minute and billions of dollars are electronically transferred around the world by banks every day.

4. Cyberspace offers enormous potential for anonymity to its members. Readily available encryption software and steganographic tools that seamlessly hide information within image and sound files ensure the confidentiality of information exchanged between cyber-citizens. 5. Cyberspace offers never-seen-before economic efficiency. Billions of dollars‖ worth of software can be traded over the Internet without the need for any government licenses, shipping and handling charges and without paying any customs duty. 6. Electronic information has become the main object of cybercrime. It is characterized by extreme mobility, which exceeds by far the mobility of persons, goods or other services. International computer networks can transfer huge amounts of data around the globe in a matter of seconds. 7. A software source code worth crores of rupees or a movie can be pirated across the globe within hours of their release. 8. Theft of corporeal information (e.g. books, papers, CD ROMs, floppy disks) is easily covered by traditional penal provisions. However, the problem begins when electronic records are copied quickly, inconspicuously and often via telecommunication facilities.

Jurisprudence of Indian Cyber Law

The primary source of cyber law in India is the Information Technology Act, 2000 (IT Act) which came into force on 17 October 2000. The primary purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government. The IT Act also penalizes various cybercrimes and provides strict punishments (imprisonment terms upto 10 years and compensation up to Rs 1 crore). An Executive Order dated 12 September 2002 contained instructions relating provisions of the Act with regard to

protected systems and application for the issue of a Digital Signature Certificate. Minor errors in the Act were rectified by the Information Technology (Removal of Difficulties) Order, 2002 which was passed on 19 September 2002. The IT Act was amended by the Negotiable Instruments (Amendments and Miscellaneous Provisions) Act, 2002. This introduced the concept of electronic cheques and truncated cheques. Information Technology (Use of Electronic Records and Digital Signatures) Rules, 2004 has provided the necessary legal framework for filing of documents with the Government as well as issue of licenses by the Government. It also provides for payment and receipt of fees in relation to the Government bodies. On the same day, the Information Technology (Certifying Authorities) Rules, 2000 also came into force. These rules prescribe the eligibility, appointment and working of Certifying Authorities (CA). These rules also lay down the technical standards, procedures and security methods to be used by a CA. These rules were amended in 2003, 2004 and 2006. Information Technology (Certifying Authority) Regulations, 2001 came into force on 9 July 2001. They provide further technical standards and procedures to be used by a CA. Two important guidelines relating to CAs were issued. The first are the Guidelines for submission of application for license to operate as a Certifying Authority under the IT Act. These guidelines were issued on 9th July 2001. Next were the Guidelines for submission of certificates and certification revocation lists to the Controller of Certifying Authorities for publishing in National Repository of Digital Certificates. These were issued on 16thDecember 2002. The Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000 also came into force on 17th October 2000. These rules prescribe the appointment and working of the Cyber Regulations Appellate Tribunal (CRAT) whose primary role is to hear appeals against orders of the Adjudicating Officers. The Cyber Regulations Appellate Tribunal (Salary, Allowances and other terms and conditions of service of Presiding Officer) Rules, 2003 prescribe the salary, allowances and other terms for the Presiding Officer of the CRAT. Information Technology (Other powers of Civil Court vested in Cyber Appellate Tribunal) Rules 2003 provided some additional powers to the CRAT. On 17th March 2003, the Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003 were passed. These rules prescribe the qualifications required for Adjudicating Officers. Their chief responsibility under the IT Act is to adjudicate on cases such as unauthorized access, unauthorized copying of data, spread of viruses, denial of service attacks, disruption of computers, computer manipulation etc. These rules also prescribe the manner and mode of inquiry and adjudication by these officers. The Government had not appointed the Adjudicating Officers or the Cyber Regulations Appellate

Tribunal for almost 2 years after the passage of the IT Act. This prompted ASCL students to file a Public Interest Litigation (PIL) in the Bombay High Court asking for a speedy appointment of Adjudicating officers. The Bombay High Court, in its order dated 9th October 2002, directed the Central Government to announce the appointment of adjudicating officers in the public media to make people aware of the appointments. The division bench of the Mumbai High Court consisting of Hon‖ble Justice A.P. Shah and Hon‖ble Justice Ranjana Desai also ordered that the Cyber Regulations Appellate Tribunal be constituted within a reasonable time frame. Following this the Central Government passed an order dated 23rd March 2003 appointing the _Secretary of Department of Information Technology of each of the States or of Union Territories' of India as the adjudicating officers. The Information Technology (Security Procedure) Rules, 2004 came into force on 29th October 2004. They prescribe provisions relating to secure digital signatures and secure electronic records. Also relevant are the Information Technology (Other Standards) Rules, 2003. An important order relating to blocking of websites was passed on 27th February, 2003. Computer Emergency Response Team (CERT-IND) can instruct Department of Telecommunications (DOT) to block a website. The Indian Penal Code (as amended by the IT Act) penalizes several cybercrimes. These include forgery of electronic records, cyber frauds, destroying electronic evidence etc. Digital Evidence is to be collected and proven in court as per the provisions of the Indian Evidence Act (as amended by the IT Act). In case of bank records, the provisions of the Bankers‖ Book Evidence Act (as amended by the IT Act) are relevant. Investigation and adjudication of cybercrimes is done in accordance with the provisions of the Code of Criminal Procedure and the IT Act. The Reserve Bank of India Act was also amended by the IT Act.

Criminal Liabilities under I.T. Act, 2000

Criminal Liability for misuse of Information Technology under Information Technology Act, 2000 are as under:

S.No.	Section	Offence Name	Description	Penalty
1.	65	Tampering with computer source document	Intentional concealment, destruction or alteration of the computer source code which is required to be kept or maintained by law	Imprisonment up to 3 years or with fine up to 2 lakh Rupees or with both.
2.	66	Hacking with Computer System	Destruction, deletion or alteration of any information residing in a computer resource, decreasing its value or utility or affecting it injuriously by whatever means intentionally or knowingly.	Imprisonment up to 3 years or with fine up to 2 lakh Rupees or with both.
3.	67	Publishing of information which is obscene in electronic form	Publication or transmission by a person or through someone else in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such which tends to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.	On first conviction with imprisonment up to 5 years and with fine up to 1 lakh Rupees and in the event of a second or subsequent conviction with imprisonment up to 10 years and also with fine up to 2 lakh Rupees.
44.	71	Misrepresentation to the Controller or the Certifying Authority	Making any misrepresentation to, or suppression of any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate, as the case may be.	Imprisonment for a term which may extend to 2 years, or with fine up to 1 lakh Rupees, or with both
55.	72	Penalty for breach of confidentiality and privacy	Any person, who, in pursuance of any of the powers conferred under IT Act, has secured access to any electronic record, book, register, correspondence, information or document without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document to any other person.	Imprisonment for a term which may extend to 2 years, or with fine up to 1 lakh Rupees, or with both.
66.	73	Publishing Digital Signature Certificate false in certain particulars	Publishing a Digital Signature Certificate or otherwise making it available to any other person with the knowledge that the Certifying Authority listed in the certificate has not issued it or the subscriber listed in the certificate has not accepted it or the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.	Imprisonment for a term which may extend to 2 years, or with fine which may extend to 1 lakh Rupees.

77.	74	Publication for fraudulent purpose	Creation, publication or otherwise making available a Digital Signature Certificate for any fraudulent or unlawful purpose.	Imprisonment for a term which may extend to 2 years, or with fine up to 1 lakh Rupees, or with both.

Offences & Penalties under the Information Technology Act, 2000

The introduction of the internet has brought the tremendous changes in our lives. People of all fields are increasingly using the computers to create, transmit and store information in the electronic form instead of the traditional papers, documents. Information stored in electronic forms has many advantages, it is cheaper, easier to store, easier to retrieve and for speedier to connection. Though it has many advantages, it has been misused by many people in order to gain themselves or for sake or otherwise to harm others. The high and speedier connectivity to the world from any place has developed many crimes and these increased offences led to the need of law for protection. Some countries have been rather been vigilant and formed some laws governing the net. In order to keep in pace with the changing generation, the Indian Parliament passed the law --- Information Technology Act 2000. The IT Act 2000 has been conceptualized on the United Nations Commissions on International Trade Law (UNCITRAL) Model Law.

The increase rate of technology in computers has led to enactment of Information Technology Act 2000. The converting of the paper work into electronic records, the storage of the electronic data, has led tremendous changed the scenario of the country. The Act further amends the Indian Penal Code, 1860, The Evidence Act, 1872, The Banker‖s Book‖s Evidence Act, 1891 and The Reserve Bank of India Act, 1934.

Offences

Cyber offences are the unlawful acts which are carried in a very sophisticated manner in which either the computer is the tool or target or both. Cybercrime usually includes:

a) Unauthorized access of the computers

b) Data diddling

c) Virus/worms attack

d) Theft of computer system

e) Hacking

f) Denial of attacks

g) Logic bombs

h) Trojan attacks

i) Internet time theft

j) Web jacking

k) Email bombing

l) Salami attacks

m) Physically damaging computer system

The offences included in the IT Act 2000 are as follows:

1. Tampering with the computer source documents.
2. Hacking with computer system.
3. Publishing of information which is obscene in electronic form.
4. Power of Controller to give directions
5. Directions of Controller to a subscriber to extend facilities to decrypt information
6. Protected system
7. Penalty for misrepresentation
8. Penalty for breach of confidentiality and privacy
9. Penalty for publishing Digital Signature Certificate false in certain particulars
10. Publication for fraudulent purpose
11. Act to apply for offence or contravention committed outside India
12. Confiscation
13. Penalties or confiscation not to interfere with other punishments.
14. Power to investigate offences.

Offences under the IT Act 2000

- ## Section 65: Tampering with computer source documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network,

when the computer source code is required to be kept or maintained by law for the being time in force, shall be punishable with imprisonment up to three year, or with fine which may extend up to two lakh rupees, or with both.

Explanation: For the purpose of this section _computer source code‘ means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

Object: The object of the section is to protect the _intellectual property‘ invested in the computer. It is an attempt to protect the computer source documents (codes) beyond what is available under the Copyright Law.

Essential ingredients of the section

1. Knowingly or intentionally concealing,
2. Knowingly or intentionally destroying,
3. Knowingly or intentionally altering,
4. Knowingly or intentionally causing others to conceal,
5. Knowingly or intentionally causing another to destroy,
6. Knowingly or intentionally causing another to alter.

This section extends towards the Copyright Act and helps the companies to protect their source code of their programmes.

Penalties: Section 65 is tried by any magistrate.

This is cognizable and non-bailable offence.

Penalties: Imprisonment up to 3 years and / or

Fine: Two lakh rupees.

Case Laws

i. Frios v/s State of Kerala

Facts: In this case it was declared that the FRIENDS application software as protected system. The author of the application challenged the notification and the constitutional validity of software under Section 70. The court upheld the validity of both.

It included tampering with source code. Computer source code the electronic form, it can be printed on paper.

Held: The court held that tampering with Source code are punishable with three years jail and or two lakh rupees fine of rupees two lakh rupees for altering, concealing and destroying the source code.

ii. Syed Asifuddin Case

Facts: In this case the Tata Indicom employees were arrested for manipulation of the electronic 32- bit number (ESN) programmed into cell phones theft were exclusively franchised to Reliance Infocom.

Held: Court held that Tampering with source code invokes Section 65 of the Information Technology Act.

iii. Parliament Attack Case

Facts: In this case several terrorist attacked on 13 December, 2001 Parliament House. In this the Digital evidence played an important role during their prosecution. The accused argued that computers and evidence can easily be tampered and hence should not be relied.

In Parliament case several smart device storage disks and devices, a Laptop were recovered from the truck intercepted at Srinagar pursuant to information given by two suspects. The laptop included the evidence of fake identity cards, video files containing clips of the political leaders with the background of Parliament in the background shot from T.V news channels. In this case design of Ministry of Home Affairs car sticker, there was game ‗wolf pack' with user name of ―Ashiq‖. There was the name in one of the fake identity cards used by the terrorist. No back up was taken therefore it was challenged in the Court.

Held: Challenges to the accuracy of computer evidence should be established by the challenger. Mere theoretical and generic doubts cannot be cast on the evidence.

- **Section66: Hacking with the computer system**

(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful 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 injuriously by any means, commits hacking.

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation: The section tells about the hacking activity.

Essential ingredients of the section:

1. Whoever with intention or knowledge.
2. Causing wrongful loss or damage to the public or any person.
3. Destroying or altering any information residing in a computer resource.
4. Or diminishes its value or utility or.

5. Affects it injuriously by any means.

Penalties: Punishment: Imprisoned up to three years and

Fine: This may extend up to two lakh rupees or with both.

Case Laws:

1. R v/s Gold & Schifreen

In this case it is observed that the accused gained access to the British telecom Prestly Gold computers networks file amount to dishonest trick and not criminal offence.

2. R v/s Whiteley.

In this case the accused gained unauthorized access to the Joint Academic Network (JANET) and deleted, added files and changed the passwords to deny access to the authorized users.

The perspective of the section is not merely protect the information but to protect the integrity and security of computer resources from attacks by unauthorized person seeking to enter such resource, whatever may be the intention or motive.

Cases Reported In India:

Official website of Maharashtra government hacked.

The official website of the government of Maharashtra was hacked by Hackers Cool Al-Jazeera, and claimed them they were from Saudi Arabia.

- ## Section 67: Publishing of obscene information in electronic form

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstance, to read see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

Essential ingredients of this section:

Publishing or transmitting, or causing to be published, pornographic material in electronic form.

Penalties: Punishment:

On first conviction- imprisonment which may extend up to five years.
Fine: up to on first conviction which may extend to one lakh rupees.
On second conviction- imprisonment up to which may extend to ten years and Fine which may extend up to two lakh rupees.

Case Laws

1. The State of Tamil Nadu v/s Suhas Katti.

Facts: This case is about posting obscene, defamatory and annoying message about a divorcee woman in the Yahoo message group. E-mails were forwarded to the victim for information by the accused through a false e- mail account opened by him in the name of the victim. These postings resulted in annoying phone calls to the lady. Based on the complaint police nabbed the accused. He was a known family friend of the victim and was interested in marrying her. She married to another person, but that marriage ended in divorce and the accused started contacting her once again. And her reluctance to marry him he started harassing her through internet.
Held: The accused is found guilty of offences under section 469, 509 IPC and 67 of IT Act 2000 and the accused is convicted and is sentenced for the offence to undergo RI for 2 years under 469 IPC and to pay fine of Rs.500/-and for the offence u/s 509 IPC sentenced to undergo 1 year Simple imprisonment and to pay fine of Rs.500/- and for the offence u/s 67 of IT Act 2000 to undergo RI for 2 years and to pay fine of Rs.4000/- All sentences to run concurrently.‘
The accused paid fine amount and he was lodged at Central Prison, Chennai. This is considered the first case convicted under section 67 of Information Technology Act 2000 in India.
In a recent case, a groom's family received numerous emails containing defamatory information about the prospective bride. Fortunately, they did not believe the emails and chose to take the matter to the police. The sender of the emails turned out to be the girl's step-father, who did not want the girl to get married, as he would have lost control over her property, of which he was the legal guardian.
2. Avnish Bajaj (CEO of bazzee.com – now a part of the eBay group of companies) case.

Facts: There were three accused first is the Delhi school boy and IIT Kharagpur Ravi Raj and the service provider Avnish Bajaj.

The law on the subject is very clear. The sections slapped on the three accused were Section 292 (sale, distribution, public exhibition, etc., of an obscene object)
and Section 294 (obscene acts, songs, etc., in a public place) of the Indian Penal Code (IPC), and Section 67 (publishing information which is obscene in electronic form) of the Information Technology Act 2000. In addition, the schoolboy faces a charge under Section 201 of the IPC (destruction of evidence), for there is apprehension that he had destroyed the mobile phone that he used in the episode. These offences invite a stiff penalty, namely, imprisonment ranging from two to five years, in the case of a first time conviction, and/or fines.
Held: In this case the Service provider Avnish Bajaj was later acquitted and the Delhi school boy was granted bail by Juvenile Justice Board and was taken into police charge and detained into Observation Home for two days.
3. DASKHINA Kannada police have solved the first case of cyber crime in the district.

A press release by Dakshina Kannada Police said here on Saturday that a Father at a Christian institution in the city had approached the Superintendent of Police with a complaint that he was getting offensive and obscene e-mails.
Police said that all the three admitted that they had done this to tarnish the image of the Father. As the three tendered an unconditional apology to the Father and gave a written undertaking that they would not repeat such act in future, the complainant withdrew his complaint. Following this, the police dropped the charges against the culprit.
The release said that sending of offensive and obscene e-mails is an offence under the Indian Information Technology Act 2000. If the charges are framed.
5.4.4 Section 68: Power of controller to give directions
 The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under.
 Any person who fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding three years or to a fine not exceeding two lakh rupees or to both.

Explanation: Any person who fails to comply with any order under sub section (1) of the above section, shall be guilty of an offence and shall be convicted for a term not less than three years or to a fine exceeding two lakh rupees or to both.

The under this section is non-bailable& cognizable.

Penalties:

Punishment: imprisonment up to a term not exceeding three years

Fine: not exceeding two lakh rupees.

- **Section 69: Directions of Controller to a subscriber to extend facilities to decrypt information**

1. If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence; for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.

2. The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information.

3. The subscriber or any person who fails to assist the agency referred to in sub section (2) shall be punished with an imprisonment for a term which may extend to seven years.

***Penalties*:** Punishment: imprisonment for a term which may extend to seven years.

The offence is cognizable and non- bailable.

- **Section 70: Protected System**

 The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system.

 The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub-section (1).

 Any person who secures access or attempts to secure access to a protected system in contravention of the provision of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

Explanation: This section grants the power to the appropriate government to declare any computer, computer system or computer network, to be a protected system. Only authorized person has the right to access to protected system.

***Penalties*:** Punishment: the imprisonment which may extend to ten years and fine.

- ## Section 71: Penalty for misrepresentation

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or which fine which may extend to one lakh rupees, or with both.

Penalties:

Punishment: imprisonment which may extend to two years

Fine: may extend to one lakh rupees or with both.

- ## Section 72: Penalty for breach of confidentiality and privacy

Save as otherwise provide in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulation made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Explanation: This section relates to any to any person who in pursuance of any of the powers conferred by the Act or it allied rules and regulations has secured access to any: Electronic record, books, register, correspondence, information, document, or other material.

If such person discloses such information, he will be punished with punished. It would not apply to disclosure of personal information of a person by a website, by his email service provider.

Penalties:

Punishment: term which may extend to two years.

Fine: one lakh rupees or with both.

- **Section 73: Penalty for publishing Digital Signature Certificate false in certain particulars**

1. No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that-

 The Certifying Authority listed in the certificate has not issued it; or

 The subscriber listed in the certificate has not accepted it; or

 The certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

2. Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Explanation: The Certifying Authority listed in the certificate has not issued it or,

The subscriber listed in the certificate has not accepted it or the certificate has been revoked or suspended.

The Certifying authority may also suspend the Digital Signature Certificate if it is of the opinion that the digital signature certificate should be suspended in public interest.

A digital signature may not be revoked unless the subscriber has been given opportunity of being heard in the matter. On revocation the Certifying Authority need to communicate the same with the subscriber. Such publication is not an offence it is the purpose of verifying a digital signature created prior to such suspension or revocation.

Penalties:

Punishment: imprisonment of a term of which may extend to two years.

Fine: fine may extend to 1 lakh rupees or with both

Case Laws:

Bennett Coleman & Co. v/s Union of India.

In this case the publication has been stated that ―publication means dissemination and circulation‖. In the context of digital medium, the term publication includes and transmission of information or data in electronic form.

- **Section 74: Publication for fraudulent purpose**

Whoever knowingly creates publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a

term which may extend to two years, or with fine which extend to one lakh rupees, or with both.

Explanation: This section prescribes punishment for the following acts:

Knowingly creating a digital signature certificate for any

 Fraudulent purpose or,

 Unlawful purpose.

Knowingly publishing a digital signature certificate for any

 Fraudulent purpose or

 Unlawful purpose

Knowingly making available a digital signature certificate for any

 Fraudulent purpose or

 Unlawful purpose.

Penalties:

Punishment: imprisonment for a term up to two years.

Fine: up to one lakh or both.

- **Section 75: Act to apply for offence or contravention committed outside India**

1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

2) For the purposes of sub-section (1), this Act shall 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.

Explanation: This section has broader perspective including cybercrime, committed by cyber criminals, of any nationality, any territoriality.

Case Laws:

R v/s Governor of Brixton prison and another.

Facts: In this case the Citibank faced the wrath of a hacker on its cash management system, resulting in illegal transfer of funds from customers account in to the accounts of the hacker, later identified as Vladimir Levin and his accomplices. After Levin was arrested he was extradite to the United States. One of the most important issues was jurisdictional issue, the ―place of origin‖ of the cybercrime.

Held: The Court held that the real- time nature of the communication link between Levin and Citibank computer meant that Levin‖s keystrokes were actually occurring on the Citibank computer.

It is thus important that in order to resolve the disputes related to jurisdiction, the issue of territoriality and nationality must be placed by a much broader criteria embracing principles of reasonableness and fairness to accommodate overlapping or conflicting interests of states, in spirit of universal jurisdiction.

- **Section 76: Confiscation**

Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provisions of this Act, rules, orders or regulations made there under has been or is being contravened, shall be liable to confiscation :

Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules orders or regulations made there under, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorized by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made there under as it may think fit.

Explanation: The aforesaid section highlights that all devices whether computer, computer system, floppies, compact disks, tape drives or any other storage, communication, input or output device which helped in the contravention of any provision of this Act, rules, orders, or regulations made under there under liable to be confiscated.

- **Section 77: Penalties or confiscation not to interfere with other punishments**

No penalty imposed or confiscation made under this Act shall prevent the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force.

Explanation: The aforesaid section lays down a mandatory condition, which states the Penalties or confiscation not to interfere with other punishments to which the person affected thereby is liable under any other law for the time being in force.

- **Section 78: Power to investigate offences**

Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Deputy Superintendent of Police shall investigate any offence under this Act.

Explanation: The police officer not below the rank of Deputy Superintendent of police shall investigate the offence.

Conclusion:

Due to the increase in the digital technology various offences has also increased. Since new-new technology come every day, the offences has also increased therefore the IT Act 2000 need to be amended in order to include those offences which are now not included in the Act. In India cybercrime is of not of high rate therefore we have time in order to tighten the cyber laws and include the offences which are now not included in the IT Act 2000.

What is ISO 27001?

ISO 27001:2013 is the international standard that provides a framework for Information Security Management Systems (ISMS) to provide continued confidentiality, integrity and availability of information as well as legal compliance. ISO 27001 certification is essential for protecting your most vital assets like employee and client information, brand image and other private information. The ISO standard includes a process-based approach to initiating, implementing, operating and maintaining your ISMS.

ISO 27001 implementation is an ideal response to customer and legal requirements such as the GDPR and potential security threats including: cyber crime, personal data breaches, vandalism / terrorism, fire / damage, misuse, theft and viral attacks.

So far in 2019, around 32 percent of businesses identified cyber security breaches or attacks in the last 12 months. The ISO 27001 standard is also structured to be compatible with other management systems standards, such as ISO 9001 and it is technology and vendor neutral, which means it is completely independent of any IT platform. As such, all members of the company should be educated on what the standard means and how it applies throughout the organization.

Achieving accredited ISO 27001 certification shows that your company is dedicated to following the best practices of information security. Additionally, ISO 27001 certification provides you with an expert evaluation of whether your organization's information is adequately protected. Read on to explore even more benefits of ISO 27001 certification.

ISO 27001 has seen a 24.7% increase in worldwide certificates in 2020, showing the growth and importance of UKAS accredited certification in recent times. Statistics straight from the most recent ISO Survey.

What Is a Security Audit?

A security audit is a comprehensive assessment of your organization's information system; typically, this assessment measures your information system's security against an audit checklist of industry best practices, externally established standards, or federal regulations. A comprehensive security audit will assess an organization's security controls relating to the following:

1. physical components of your information system and the environment in which the information system is housed.
2. applications and software, including security patches your systems administrators have already implemented.
3. network vulnerabilities, including evaluations of information as it travels between different points within, and external of, your organization's network
4. the human dimension, including how employees collect, share, and store highly sensitive information.

How Does a Security Audit Work?

A security audit works by testing whether your organization's information system is adhering to a set of internal or external criteria regulating data security. Internal criteria includes your company's IT policies and procedures and security controls. External criteria include federal regulations like the Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley Act (SOX), and standards set by the International Organization for Standardization (ISO) or the National Institute for Standards in Technology (NIST). A security audit compares your organization's actual IT practices with the standards relevant to your enterprise, and will identify areas for remediation and growth.

What Is the Main Purpose of a Security Audit? Why Is It Important?

A security audit will provide a roadmap of your organization's main information security weaknesses and identify where it is meeting the criteria the organization has set out to follow and where it isn't. Security audits are crucial to developing risk assessment plans and mitigation strategies for organizations that deal with individuals' sensitive and confidential data.

Benefits of IT Security Audit

Like we mentioned, an IT security audit reveals underlying vulnerabilities and security risks in an organization's IT assets. Identifying risks, however, has a positive rippling effect on the organization's overall security. How? We discuss them point by point below:

1. **Weighs your current security structure** and protocols and helps you define a standard for your organization with the audit results.
2. **Mitigates hacker-risks** by discovering potential hacker entry points and security flaws well in advance.
3. **Verifies how compliant your IT infrastructure is** with top regulatory bodies and helps you conform in accordance.
4. **Finds lag in your organization's security training and awareness** and helps you make informed decisions towards its betterment.

Types of IT Security Audit

There is more than one way to categorize an IT security audit. Generally, it's been categorized on the basis of approach, methodology, etc. Some of the common categorizations are:

Approach Based

- **Black Box Audit:** Here, the auditor only knows about the info that is publicly available regarding the organization that is to be audited.
- **White Box Audit:** In this type of security audit, the auditor is provided with detailed info (i.e. source code, employee access, etc) regarding the organization that is to be audited.
- **Grey Box Audit:** Here, the auditor is provided with some info, to begin with, the auditing process. This info can also be gathered by the auditors themselves but is provided to save time.

Methodology Based

- **Penetration Tests:** The auditor tries to break into the organization's infrastructure.
- **Compliance Audits:** Only certain parameters are checked to see if the organization is complying with security standards.
- **Risk Assessments:** An analysis of critical resources that may be threatened in case of a security breach.
- **Vulnerability Tests:** Necessary scans are performed to find possible security risks. Many false positives may be present.
- **Due Diligence Questionnaires:** Used for an analysis of existing security standards in the organization.

Importance of an IT security audit

- Protects the critical data resources of an organization.
- Keeps the organization compliant to various security certifications.
- Identifies security loopholes before the hackers.
- Keeps the organization updated with security measures.
- Identifies physical security vulnerabilities.
- Helps in formulating new security policies for the organization.
- Prepares the organization for emergency response in case of a cybersecurity breach.

Intellectual Property in Cyberspace

Intellectual Property (IP) simply refers to the creation of the mind. It refers to the possession of thought or design by the one who came up with it. It offers the owner of any inventive design or any form of distinct work some exclusive rights, that make it unlawful to copy or reuse that work without the owner's permission. It is a part of property law. People associated with literature, music, invention, etc. can use it in business practices.

There are numerous types of tools of protection that come under the term "intellectual property". Notable among these are the following:

- Patent
- Trademark
- Geographical indications
- Layout Designs of Integrated Circuits
- Trade secrets
- Copyrights
- Industrial Designs

Cyberspace is the non-physical domain where numerous computers are connected through computer networks to establish communication between them. With the expansion of technology, cyberspace has come within reach of every individual. This fact led to the emergence of cyberspace as a business platform and hence increases pressure on Intellectual

Property. Nowadays, cyber crimes do not solely limit themselves to fraud, cyberbullying, identity thefts but also an infringement of copyrights and trademarks of various businesses and other organizations. Online content needs to be protected and hence Intellectual Property Rights and Cyber laws cannot be separated.

In cyberspace, sometimes one person makes a profit by using another person's creation without the owner's consent. This is a violation of privacy, and it is protected by IPR. We have certain laws to avoid violation of Intellectual Property Rights in cyberspace and when it is violated, then additionally we have several remedies in law.

Copyright Infringement:

Copyright protection is given to the owner of any published artistic, literary, or scientific work over his work to prohibit everyone else from exploiting that work in his name and thereby gain profit from it.

When these proprietary creations are utilized by anyone without the permission of the owner, it leads to copyright infringement. If copies of any software are made and sold on the internet without the permission of the owner or even copying the content from any online source, these all are examples of copyright infringement.

Copyright Issues in Cyberspace :

1. Linking – It permits a Website user to visit another location on the Internet. By simply clicking on a word or image on one Web page, the user can view another Web page elsewhere in the world, or simply elsewhere on the same server as the original page.

Linking damages the rights or interests of the owner of the Linked webpage. It may create the supposition that the two linked sites are the same and promote the same idea. In this way, the linked sites can lose their income as it is often equal to the number of persons who visit their page.

2. Software Piracy – Software piracy refers to the act of stealing software that is lawfully shielded. This stealing comprises various actions like copying, spreading, altering, or trading the software. It also comes under the Indian copyright act.

An example of software piracy is downloading a replica of Microsoft Word from any website other than Microsoft to avoid paying for it as it is a paid software. Piracy can be of 3 types:

1. Soft lifting
2. Software Counterfeiting
3. Uploading-Downloading.

3. Cybersquatting – Cybersquatting means unauthorized registration and use of Internet domain names that are similar to any business's trademarks, service marks, or company names. For example, let us consider Xyz is a very famous company and the company hadn't created a website yet. A cybersquatter could buy xyz.com, looking to sell the domain to the company Xyz at a later date for a profit. The domain name of a famous company can even be used to attract traffic and this traffic will help cybersquatters earn a lot of money through advertising.

When more than one individual believes that they have the right to register a specific domain name, then this can lead to a Domain Name Dispute. It arises when a registered trademark is registered by another individual or organization who is not the owner of a trademark that is registered.

Trademark Issues in Cyberspace : Trademark means a mark capable of being depicted diagrammatically and which may distinguish the products or services of one person from those of others and will embody the form of products, their packaging, and combination of colors. A registered service mark represents a service. Trademark infringement refers to the unlawful use of a trademark or service mark which can cause ambiguity, fraud, or confusion about the actual company a product or service came from. Trademark owners can take the help of the law if they believe their marks are being infringed.