10
TECHNOLOGY REVOLUTION AND ITS IMPACT ON LEGAL ENVIRONMENT "ADVANCE TECHNOLOGY AND LAWS"

Neha Singh
Asst. Professor, HOD (Professor), IMS LAW College
Dr. Niti Sihna
Asst. Professor, HOD (Professor), IMS LAW College

Abstract
Looking at the present scenario one can easily predict the dominance of technology revolution. Globalization and liberalization has expanded their wings in the cyber world and this expansion now leads towards the growth of cyber crime . We can bring revolution in technology with the help of globalised technology. As we enter into the globalised world we are actually entering into the time of advance technology. Technology is not always good for us sometimes it is having some bad effect also. Without technology we cannot progress ourselves. So advancement of technology is must but at the same time due to changes in the situations we have to take care, that , no one can misuse these technology .For doing this the best method which we can opt is to make laws on these advanced technology so that technology can be protected . As the society advances it requires changes and accordingly we have to change our laws also. With time we have to make laws very strict and adjustable according to the prevailing situations. Internet is one the best tool through which we can globalise our techniques. Internet is providing us the best means to get any information on any topic . But it is harmful also .As there are various hackers who always try to hack the account of any person to harm them Now a day's crime is not only of criminal and civil nature but now it is technical in nature. Previous laws are not sufficient enough to get rid of it , so that we need some specific laws which provides protection to common man. As we are in favor of cashless society and for that we have to be dependent upon internet so we have to make ourselves aware about the precautionary measures through which we can avail the remedy if something happens wrong. Globisation is all about the advancement of technology with this we have to change our legal environment also.
In this research paper basically we are focusing upon the laws which provides protection from the crime which creates hurdles in making our country an advanced developed globalised country.

Keywords: Technology Revolution, Legal Environment, Criminal and Civil Nature, Globalization, Hackers, Interconnected, Techniques

INTRODUCTION

Technology is the collection of techniques, skills, methods and processes used in the production of goods or services or in the accomplishment of objectives, such as scientific investigation.

The human species' use of technology began with the conversion of natural resources into simple tools.

Technology has many effects. It has helped develop more advanced economies (including today's global economy) and has allowed the rise of a leisure class. Many technological processes produce unwanted by-products known as pollution and deplete natural resources to the detriment of Earth's environment. Various implementations of technology influence the values of a society and new technology often raises new ethical questions. Examples include the rise of the notion of efficiency in terms of human productivity, a term originally applied only to machines, and the challenge of traditional norms.

USE OF TECHONOLOGY

1. **Use of technology in business:**
   Today businesses can save money by using technology to perform certain tasks. When you compare the amount of money spent on hiring an individual to perform a certain task and to guarantee delivery on time, it is totally expensive. When it comes to technology a small business can scale out and deliver more with less human resource.
2. **The Use of technology in communication:**
   Unlike in the past when communication was limited to letter writing and waiting for those postal services to deliver your message. Today technology has made the field of communications so easy. Now you can draft a business message and email it or fax in a second without any delays, the recipient will get the message an they will reply you instantly.
3. **Use of technology in human relationships:**
   As the world develops, people are getting more carried away with their work and carries. Today a lot is demanded so every one is busy to have time to find a relationship. So technology has also filled this part.

With technology you can connect and meet new people while at work using social network technology. You can also use technology to find a new date without living your work. Now days people use mobile phone apps to meet and connect with new and old friends. Social networks like Facebook. com , Tagged.com have played a big role in connecting both old and new relationships.

4. **Use of technology in education:**
Today, technology has made a very big change in the education world. With the invention of technological gadgets and mobile apps which helps students learn easily. Now days you can access a full library via a mobile app on any smart phone or ipad. Before inventing this technology, students had to go to physical libraries to get the information they need. some of these library Apps include

5. **Use of technology in purchasing:**
Technology has also made the buying and selling of good so flexible. With the introduction e-payment systems like Paypal.com and Square Wallet App , users can easily purchase any thing online without living the comfort of their homes.

6. **The Use of technology in agriculture:**
With the invention of Mobile App for farmers, they can use an App like ”FamGraze” to work faster and be more accurate while in the field and off the field. For example, ”FamGraze” app will help a farmer manage their grass more effectively by suggesting the cheapest feed for their livestock. This app will calculate the amount of grass your animals have in the field. You will need no paper or any spreadsheets to do all this. Saving you more time while in the field.

7. **Use of technology in banking:**
Now electronic banking moving money has become so simple. The invention of VISA ELECTRON has made it simple to move with more money with out having any fears of getting robbed on the way. You can buy any thing with a Visa Electron card, so in this case you don’t have to move with cash.

8. **Use of technology to control and harness natural forces:**
Natural forces affect and disrupt human life and daily economic activates. For example; Floods wash away farmland and homes, they carry out fertile top soil and disrupt the growth of crops. Also fires burn buildings, crops and forests which affect human life. However, technology has enabled humans build large dams which can harbor excess water and use that water to generate power. Also fire is tamed to heat our homes and process industrial materials. Wind is being used to generate electricity. We have converted solar energy to power which is being used in homes and businesses. All this is a result of using technology to control natural forces.

9. **Use of technology in transportation:**
Transportation is one of the basic areas of technological activity.Both businesses and individuals have benefited from the new technologies in the travel industry. Time is money , so we must have first and efficient means of transport. Try to imagine life without well developed transportation systems. I think of transportation in the same light as food, clothing and shelter. It has become a basic need , because we use advanced transport means like cars , trains , airplanes to go to work , to transport goods , to go shopping, to visit friends and families and so much more.

REVOLUTION IN TECHNOLOGY

So we have seen there are various uses of technology. As technology gets advane problems are also there with the technology . Its very easy to handle all techniques but its not easy once problem arises with it . If certain problem are there in the uses of technology to sovle this problem we are havint it experts but if any wrong act is being involved in that to stop the crime we have to take help of laws . Laws should be very strict then only these crimes will be stopped

As we seen so many of terrorist attacts whrer errorist uses the hi techqe technology to attack on difeernt differtn countries . Its revolution can change the world at the same time its revolution can destroy the world also;

1. **Law firms are making a greater investment in IT.**
Nearly six in 10 (59 percent) lawyers interviewed for the Future Law Office project said their law firms will increase spending on technology in the next two years. Law firms plan to purchase software (79percent), hardware (72 percent), desktop PCs (62 percent), laptops (49 percent), tablet PCs or handheld computers (44 percent) and smartphones (41 percent).

2. **Web-based tools are improving client communication and the delivery of legal services.**
Lawyers surveyed said their law firms used e-filing systems (83 percent), meeting or audio-conferencing tools (79 percent), document storage sites (58 percent), collaborative or information-sharing sites (51 percent) and client portals or extranets (30 percent).
   - Law firms’ office footprint is shrinking. With mobile devices and wireless networks enabling lawyers to work remotely from any location, law firms are reducing the size of their offices and reconfiguring workspaces.

3. **Technology is leveling the playing field.**
With firms of all sizes now using

similar products, services and tools, small firms and solo practitioners are able to establish a bigger presence online and, in some cases, better compete with larger firms.

4. **Corporate legal departments are using tech tools to manage higher workloads.**
   Nearly one in three in-house counsel (30 percent) interviewed said their legal department's greatest challenge is reducing budgets/controlling costs. They are utilizing technology solutions to streamline communications with outside counsel and improve efficiencies.
5. **Technology has dramatically changed the realm of discovery.**
   As the amount of electronic data grows exponentially,e-discovery remains both a growth area and a challenge for law firms and their corporate clients.

Law Firms Take a Strategic Approach to Technology

"Technology has changed the practice of law – from the way legal teams prepare for trial and present cases, to how they communicate with clients and colleagues," said Charles Volkert, executive director of Robert Half Legal. "Knowledge-sharing platforms, portals and intranets are being used by an increasingly mobile legal workforce. These systems, along with laptops, tablet computers and smartphones, have become essential to law firm productivity."

A growing number of firms are marketing their professional services to different audiences via social media, the research found. However, law firms using these online networks, as well as cloud computing-based services to store data, must address new privacy concerns regarding the security of privileged information. This has prompted many firms to allocate additional resources toward protecting their systems and safeguarding confidential data.

Corporate Legal Departments Use Technology to Reduce Costs

Software designed to monitor expenses and improve the work process is gaining in popularity among corporate legal departments, the research showed. "Many companies are using project management tools to track spending, and streamlining workflow with group calendaring and online collaboration tools," Volkert said.

Technology is influencing the type of work being assigned to outside counsel, as well. "While litigation and e-discovery projects are typically outsourced, if internal teams have access to the same software programs and systems as their law firms, general counsel might keep certain matters in-house to contain costs," Volkert said.

REASONS FOR CYBERCRIME: PROBLEMS

1. Capacity to store data in comparatively small space:-
2. Easy to access:-
3. Complex-
4. Negligence:-
5. Â Loss of evidence:-

COMMON CYBER-CRIME SCENARIOS AND APPLICABILITY OF LEGAL SECTIONS

Cyber-crime scenarios which can attract prosecution as per the penalties and offences prescribed in IT Act 2000 (amended via 2008) Ac

Harassment via fake public profile on social networking site

A fake profile of a person is created on a social networking site with the correct address, residential information or contact details but he/she is labelled as 'prostitute' or a person of 'loose character'. This leads to harassment of the victim.Provisions Applicable:- Sections 66A, 67 of IT Act and Section 509 of the Indian Penal Code.

Online Hate Community

Online hate community is created inciting a religious group to act or pass objectionable remarks against a country, national figures etc.Provisions Applicable: Section 66A of IT Act and 153A & 153B of the Indian Penal Code.

Email Account Hacking

If victim's email account is hacked and obscene emails are sent to people in victim's address book.Provisions Applicable:- Sections 43, 66, 66A, 66C, 67, 67A and 67B of IT Act.

Credit Card Fraud

Unsuspecting victims would use infected computers to make online transactions. Provisions Applicable:- Sections 43, 66, 66C, 66D of IT Act and section 420 of the IPC.

Web Defacement

The homepage of a website is replaced with a pornographic or defamatory page. Government sites generally face the wrath of hackers on symbolic days.Provisions Applicable:- Sections 43 and 66 of IT Act and Sections 66F, 67 and 70 of IT Act also apply in some cases.

Introducing Viruses, Worms, Backdoors, Rootkits, Trojans, Bugs

All of the above are some sort of malicious programs which are used to destroy or gain access to some electronic information. Provisions Applicable:- Sections 43, 66, 66A of IT Act and Section 426 of Indian Penal Code.

Cyber Terrorism

Many terrorists are use virtual(GDrive, FTP sites) and physical storage media(USB's, hard drives) for hiding information and records of their illicit business.Provisions Applicable: Conventional terrorism laws may apply along with Section 69 of IT Act.

Online sale of illegal Articles
Where sale of narcotics, drugs weapons and wildlife is facilitated by the InternetProvisions Applicable:- Generally conventional laws apply in these cases.

Cyber Pornography
Among the largest businesses on Internet. Pornography may not be illegal in many countries, but child pornography is.Provisions Applicable:- Sections 67, 67A and 67B of the IT Act.

Phishing and Email Scams
Phishing involves fraudulently acquiring sensitive information through masquerading a site as a trusted entity. (E.g. Passwords, credit card information)Provisions Applicable:- Section 66, 66A and 66D of IT Act and Section 420 of IPC

Theft of Confidential Information
Many business organizations store their confidential information in computer systems. This information is targeted by rivals, criminals and disgruntled employees. Provisions Applicable:- Sections 43, 66, 66B of IT Act and Section 426 of Indian Penal Code.

Source Code Theft
A Source code generally is the most coveted and important "crown jewel" asset of a company.Provisions applicable:- Sections 43, 66, 66B of IT Act and Section 63 of Copyright Act.

Tax Evasion and Money Laundering
Money launderers and people doing illegal business activities hide their information in virtual as well as physical activities. Provisions Applicable: Income Tax Act and Prevention of Money Laundering Act. IT Act may apply case-wise.

Online Share Trading Fraud
It has become mandatory for investors to have their demat accounts linked with their online banking accounts which are generally accessed unauthorized, thereby leading to share trading frauds.Provisions Applicable: Sections 43, 66, 66C, 66D of IT Act and Section 420 of IPC

LAWS MADE FOR THE PROTECTION OF TECHNOLOGY

IT legislation in India
The Government of India enacted its Information Technology Act 2000 with the objectives stating officially as:
"to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."

Notable features of the ITAA 2008 are:
- Focusing on data privacy
- Focusing on Information Security
- Defining cyber café
- Making digital signature technology neutral
- Defining reasonable security practices to be followed by corporate
- Redefining the role of intermediaries
- Recognizing the role of Indian Computer Emergency Response Team
- Inclusion of some additional cyber crimes like child pornography and cyber terrorism
- Authorizing an Inspector to investigate cyber offenses (as against the DSP earlier)

What is a cyber crime?
Cyber Crime is not defined officially in IT Act or in any other legislation. In fact, it cannot be too. Offence or crime has been dealt with elaborately listing various acts and the punishments for each, under the Indian Penal Code, 1860 and related legislations. Hence, the concept of cyber crime is just a "combination of crime and computer".

Cases Studies as per selected IT Act Sections
Section 43 – Penalty and Compensation for damage to computer, computer system, etc

Related Case: Mphasis BPO Fraud: 2005 In December 2004, four call centre employees, working at an outsourcing facility operated by MphasiS in India, obtained PIN codes from four customers of MphasiS' client, Citi Group. These employees were not authorized to obtain the PINs. In association with others, the call centre employees opened new accounts at Indian banks using false identities. Within two months, they used the PINs and account information gleaned during their employment at MphasiS to transfer money from the bank accounts of CitiGroup customers to the new accounts at Indian banks.

By April 2005, the Indian police had tipped off to the scam by a U.S. bank, and quickly identified the individuals involved in the scam. Arrests were made when those individuals attempted to withdraw cash from the falsified accounts, $426,000 was stolen; the amount recovered was $230,000.

Verdict: Court held that Section 43(a) was applicable here due to the nature of unauthorized access involved to commit transactions.

Section 65 – Tampering with Computer Source Documents
Related Case: Syed Asifuddin and Ors. Vs. The State of Andhra Pradesh In this case, Tata Indicom employees were arrested for manipulation of the electronic 32- bit number (ESN) programmed into cell phones

theft were exclusively franchised to Reliance Infocomm.

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

Section 66 – Computer Related offenses
Related Case: Kumar 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.Investigations had revealed that Kumar was logging on to the BSNL broadband Internet connection as if he was the authorized genuine user and 'made alteration in the computer database pertaining to broadband Internet user accounts' of the subscribers.The CBI had registered a cyber crime case against Kumar and carried out investigations on the basis of a complaint by the Press Information Bureau, Chennai, which detected the unauthorised use of broadband Internet. The complaint also stated that the subscribers had incurred a loss of Rs 38,248 due to Kumar's wrongful act. He used to 'hack' sites from Bangalore, Chennai and other cities too, they said.

Verdict: The Additional Chief Metropolitan Magistrate, Egmore, Chennai, sentenced N G Arun Kumar, the techie from Bangalore to undergo a rigorous imprisonment for one year with a fine of Rs 5,000 under section 420 IPC (cheating) and Section 66 of IT Act (Computer related Offense).

Section 66A – Punishment for sending offensive messages through communication service
Relevant Case #1: Fake profile of President posted by imposter On September 9, 2010, the imposter made a fake profile in the name of the Hon'ble President Pratibha Devi Patil. A complaint was made from Additional Controller, President Household, President Secretariat regarding the four fake profiles created in the name of Hon'ble President on social networking website, Facebook.The said complaint stated that president house has nothing to do with the facebook and the fake profile is misleading the general public. The First Information Report Under Sections 469 IPC and 66A Information Technology Act, 2000 was registered based on the said complaint at the police station, Economic Offences Wing, the elite wing of Delhi Police which specializes in investigating economic crimes including cyber offences.

Relevant Case #2: Bomb Hoax mail In 2009, a 15-year-old Bangalore teenager was arrested by the cyber crime investigation cell (CCIC) of the city crime branch for allegedly sending a hoax e-mail to a private news channel. In the e-mail, he claimed to have planted five bombs in Mumbai, challenging the police to find them before it was too late. At around 1p.m. on May 25, the news channel received an e-mail that read: "I have planted five bombs in Mumbai; you have two hours to find it." The police, who were alerted immediately, traced the Internet Protocol (IP) address to Vijay Nagar in Bangalore. The Internet service provider for the account was BSNL, said officials.

Section 66D – Punishment for cheating by impersonation by using computer resource
Relevant Case: Sandeep Vaghese v/s State of Kerala
A complaint filed by the representative of a Company, which was engaged in the business of trading and distribution of petrochemicals in India and overseas, a crime was registered against nine persons, alleging offenses under Sections 65, 66, 66A, C and D of the Information Technology Act along with Sections 419 and 420 of the Indian Penal Code.

The company has a web-site in the name and and style `www.jaypolychem.com' but, another web site `www.jayplychem.org' was set up in the internet by first accused Samdeep Varghese @ Sam, (who was dismissed from the company) in conspiracy with other accused, including Preeti and Charanjeet Singh, who are the sister and brother-in-law of `Sam'

Defamatory and malicious matters about the company and its directors were made available in that website. The accused sister and brother-in-law were based in Cochin and they had been acting in collusion known and unknown persons, who have collectively cheated the company and committed acts of forgery, impersonation etc.

Two of the accused, Amardeep Singh and Rahul had visited Delhi and Cochin. The first accused and others sent e-mails from fake e-mail accounts of many of the customers, suppliers, Bank etc. to malign the name and image of the Company and its Directors. The defamation campaign run by all the said persons named above has caused immense damage to the name and reputation of the Company.

The Company suffered losses of several crores of Rupees from producers, suppliers and customers and were unable to do business.

Section 66E – Punishment for violation of privacy
Relevant Cases:
Jawaharlal Nehru University MMS scandal In a severe shock to the prestigious and renowned institute – Jawaharlal Nehru University, a pornographic MMS clip was apparently made in the campus and transmitted outside the university.Some media reports claimed that the two accused students initially tried to extort money from the girl in the video but when they failed the culprits put the video out on mobile phones, on the internet and even sold it as a CD in the blue film market.

Nagpur Congress leader's son MMS scandal On January 05, 2012 Nagpur Police arrested two engineering students, one of them a son

of a Congress leader, for harassing a 16-year-old girl by circulating an MMS clip of their sexual acts. According to the Nagpur (rural) police, the girl was in a relationship with Mithilesh Gajbhiye, 19, son of Yashodha Dhanraj Gajbhiye, a zila parishad member and an influential Congress leader of Saoner region in Nagpur district.

Section-66F Cyber Terrorism

Relevant Case: The Mumbai police have registered a case of 'cyber terrorism'—the first in the state since an amendment to the Information Technology Act—where a threat email was sent to the BSE and NSE on Monday. The MRA Marg police and the Cyber Crime Investigation Cell are jointly probing the case. The suspect has been detained in this case.The police said an email challenging the security agencies to prevent a terror attack was sent by one Shahab Md with an ID sh.itaiyeb125@yahoo.in to BSE's administrative email ID corp.relations@bseindia.com at around 10.44 am on Monday.The IP address of the sender has been traced to Patna in Bihar. The ISP is Sify. The email ID was created just four minutes before the email was sent. "The sender had, while creating the new ID, given two mobile numbers in the personal details column. Both the numbers belong to a photo frame-maker in Patna," said an officer.

Status: The MRA Marg police have registered forgery for purpose of cheating, criminal intimidation cases under the IPC and a cyber-terrorism case under the IT Act.

Section 67 – Punishment for publishing or transmitting obscene material in electronic form

Relevant Case: 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 lady's complaint, the police nabbed the accused.Investigation revealed that he was a known family friend of the victim and was interested in marrying her. She was married to another person, but that marriage ended in divorce and the accused started contacting her once again. On her reluctance to marry him he started harassing her through internet.

Verdict: The accused was found guilty of offences under section 469, 509 IPC and 67 of IT Act 2000. He is convicted and sentenced for the offence as follows:

As per 469 of IPC he has to undergo rigorous imprisonment for 2 years and to pay fine of Rs.500/-

As per 509 of IPC he is to undergo to undergo 1 year Simple imprisonment and to pay Rs 500/-

As per Section 67 of IT Act 2000, he has to undergo for 2 years and to pay fine of Rs.4000/-

All sentences were 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.

Section 67B – Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form

Relevant Case: Janhit Manch & Ors. v. The Union of India 10.03.2010 Public Interest Litigation: The petition sought a blanket ban on pornographic websites. The NGO had argued that websites displaying sexually explicit content had an adverse influence, leading youth on a delinquent path.

Section 69 – Powers to issue directions for interception or monitoring or decryption of any information through any computer resource

Relevant Case: In August 2007, Lakshmana Kailash K., a techie from Bangalore was arrested on the suspicion of having posted insulting images of Chhatrapati Shivaji, a major historical figure in the state of Maharashtra, on the social-networking site Orkut.The police identified him based on IP address details obtained from Google and Airtel -Lakshmana's ISP. He was brought to Pune and detained for 50 days before it was discovered that the IP address provided by Airtel was erroneous. The mistake was evidently due to the fact that while requesting information from Airtel, the police had not properly specified whether the suspect had posted the content at 1:15 p.m.

Verdict: Taking cognizance of his plight from newspaper accounts, the State Human Rights Commission subsequently ordered the company to pay Rs 2 lakh to Lakshmana as damages. The incident highlights how minor privacy violations by ISPs and intermediaries could have impacts that gravely undermine other basic human rights.

PENALTIES, COMPENSATION AND ADJUDICATION SECTIONS

Section 43 – Penalty and Compensation for damage to computer, computer system

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

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

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

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

Damages or causes to be damaged any computer, computer system or computer network, data, computer database, or any other programmes residing in such computer, computer system or computer networkDisrupts or causes disruption of any computer, computer system, or computer network;

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

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

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

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

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

Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage,he shall be liable to pay damages by way of compensation to the person so affected.

Section 43A – Compensation for failure to protect data Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, not exceeding five crore rupees, to the person so affected.

Section 44 – Penalty for failure to furnish information or return, etc. If any person who is required under this Act or any rules or regulations made there under to –
Furnish any document, return or report to the Controller or the Certifying Authority, fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;

File any return or furnish any information, books or other documents within the time specified therefore in the regulations, fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues:

Maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

Section 45 – Residuary Penalty Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided,shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

Section 47 – Factors to be taken into account by the adjudicating officer Section 47 lays down that while adjudging the quantum of compensation under this Act, an adjudicating officer shall have due regard to the following factors, namely :-

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

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

The repetitive nature of the default.

Offences Sections

Section 65 – Tampering with Computer Source Documents If any person knowingly or intentionally conceals, destroys code or alters or causes another to conceal, destroy code or alter any computer, computer program, computer system, or computer network,he shall be punishable with imprisonment up to three years, or with fine up to two lakh rupees, or with both.

Section – 66 Computer Related Offences If any person, dishonestly, or fraudulently, does any act referred to in section 43,he shall be punishable with imprisonment for a term which may extend to two three years or with fine which may extend to five lakh rupees or with both.

Section 66A – Punishment for sending offensive messages through communication service Any person who sends, by means of a computer resource or a communication device,

Any information that is grossly offensive or has menacing character;

Any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes by making use of such computer resource or a communication device,

Any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin

of such messages shall be punishable with imprisonment for a term which may extend to three years and with fine.

Section 66B – Punishment for dishonestly receiving stolen computer resource or communication device. Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device,shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

Section 66C – Punishment for identity theft Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person,shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Section 66D – Punishment for cheating by personation by using computer resource Whoever, by means of any communication device or computer resource cheats by personating; shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Section 66E – Punishment for violation of privacy Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, Explanation – For the purposes of this section:

"transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons;

"capture", with respect to an image, means to videotape, photograph, film or record by any means;

"private area" means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

"publishes" means reproduction in the printed or electronic form and making it available for public;

"under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that–
he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

Section-66F Cyber Terrorism
Whoever,- with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

denying or cause the denial of access to any person authorized to access computer resource; or

attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or

introducing or causing to introduce any Computer Contaminant and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or

knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

Section 67 – Punishment for publishing or transmitting obscene material 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 circumstances, 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 two three years and with fine which may extend to five lakh rupees andin 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.

Section 67A – Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conductshall 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 ten lakh rupees andin 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.

Section 67B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form Whoever:-

publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or

creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or

cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or

facilitates abusing children online or

records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,

shall be punished on first conviction with imprisonment of either description 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:

Provided that the provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form

Section 69 – Powers to issue directions for interception or monitoring or decryption of any information through any computer resource.-

Where the central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if is satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resource.

The Procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

The subscriber or intermediary 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 –

provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or

intercept or monitor or decrypt the information, as the case may be; or

provide information stored in computer resource.

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

Section 69A – Power to issue directions for blocking for public access of any information through any computer resource

Where the Central Government or any of its officer specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-sections (2) for reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource.

The procedure and safeguards subject to which such blocking for access by the public may be carried out shall be such as may be prescribed.

The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.

Section 69B. Power to authorize to monitor and collect traffic data or information

through any computer resource for Cyber Security
The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.

Any intermediary who intentionally or knowingly contravenes the provisions of subsection (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to 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 Electronic Signature Certificate, as the case may be,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.

Section 72 – Breach of confidentiality and privacy Any person who, in pursuant of any of the powers conferred under this Act, rules or regulations 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 electronic record, book, register, correspondence, information, document or other 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.

Section 72A – Punishment for Disclosure of information in breach of lawful contract
Any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

Section 73. Penalty for publishing electronic Signature Certificate false in certain particulars.
No person shall publish a Electronic 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

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.

Section 74 – Publication for fraudulent purpose: Whoever knowingly creates, publishes or otherwise makes available a Electronic 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 may extend to one lakh rupees, or with both.

Section 75 – Act to apply for offence or contraventions committed outside India
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.

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.

Section 77A – Compounding of Offences.
A Court of competent jurisdiction may compound offences other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided under this Act. Provided further that the Court shall not compound any offence where such offence affects the socio-economic conditions of the country or has been committed against a child below the age of 18 years or a woman.

The person accused of an offence under this act may file an application for compounding in the court in which offence is pending for trial and the provisions of section 265 B and 265C of Code of Criminal Procedures, 1973 shall apply.

Section 77B – Offences with three years imprisonment to be cognizable
Notwithstanding anything contained in Criminal Procedure Code 1973, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable.

Section 78 – Power to investigate offences
Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Inspector shall investigate any offence under this Act.

SUGGESTIONS :

- Where do we draw the line on what is legal—and ethical?
- Awareness
- To use technology with proper security
- Co-operate with the authority
- Don't be impatience

REFERENCES:

1. *Information and Technology Act ,2000 – Bare Act*
2. *Information and Technology Act , 2008 Amendment*
3. *CYBER LAW - The Indian Perspective : PavanDuggal (Advocate)*
4. *Legal Framework on CYBER CRIMES : K.Mani (Advocate)*
5. *Cyber LawsJustice :Yatindra Singh*
6. *Law & Emerging Technology (Cyber Law) : HemantGoel*
7. *Cyber Law-Law Of Information Technology And Internet:Anirudh Rastogi*
8. *Bare Act of Information and technology Act ,2000*
9. *http://www.prnewswire.com*
10. *https://www.ukessays.com*
11. *http://www.brainyquote.com/words/cr/crime149615.html#ixzz1h5KlT6p*
12. *http://www.crimeresearch.org/articles/joseph06/.*
13. *http://cis-India.org/internetovernance/publications/it-act/short-note-on-amendment-act-2008*
14. *http://niiconsulting.com/checkmate/2014/06/it-act-2000-penalties-offences-with case-studies.*