VOLUME 6 ISSN 2456-9704

DIGITAL REVOLUTION: LEGAL METHODOLOGY ON COMPUTERS AND INTERNET

By *Gunish Aggarwal*
From *Chanderprabhu Jain College of Higher Studies and School of law, New Delhi*

ABSTRACT
It is necessary to explore the links between law and technological development, the different paces of changes in each other and resulting gaps between them. It is necessary to examine the structural effects of information technology on the legal rules that aim to regulate this area. As we know, law has followed significant changes in the mind and culture. The range of emerging technologies has changed the society. The technology has progressed to such an extent that it has had a considerable impact on both society and politics. In the past few decades there has been a revolution in computing and communications and all indications are that technological progress and the use of information technology will continue at a rapid pace. We need to understand the ethical considerations of technological innovations. It is necessary to understand the impacts of information technology and E- Commerce, E-Contracting, Electronic Money, Electronic Signatures, Electronic Evidence and Cyber Crimes. The timely necessity to understand the emerging issues on internet need to be carefully analysed. With the emergence of technology, the concept of Online Dispute Resolution has gained light. Not only these areas of technology, but the area of Law and Medicine needs to be carefully studied. Therefore high- potential, high-risks emerging technologies present a social and regulatory quandary. The development and governance of such technologies are inevitably and dynamically intertwined. A technology cannot advance without freedom of research and development, but too much freedom can lead to a technological calamity that will become difficult to overcome.If we analyse the concepts historically, we learn that advancement in technology has posed challenges before the society, for example,'digital divide.' Therefore we need to understand the different Legislations of different countries and learn how much are they effective to overcome the challenges posed.

Keywords: Cyber Crimes,Electronic Commerce, Law and Medicine, Law and Technology, Online Dispute Resolution

INTRODUCTION

Is an innovation and technology related theory that describes radical transformation of society through technological development. Richta defines technology as "a material entity created by the application of mental and physical effort to nature in order to achieve some value" evolves in three stages[1]. These are tools, machine and automation. The evolution of technology can be divided into two trends that is Development and Theoretical Implications.

- Development:
The pre-technological period, in which all other animal species remain today aside from some avian and primate species was a non-rational period of the early prehistoric

[1]See A View of the Distant Past, the Present and the Far Future, Masefield Books, 1993

man. The emergence of technology, made possible by the development of the rational faculty, paved the way for the first stage: the tool. The tool provides a mechanical advantage in accomplishing a physical task, such as an arrow, plough or hammer that arguments physical labour to more efficiently achieve his objective. Later animal-powered tools such as the plow and the horse, increased the productivity of food production about tenfold over the technology over the technology of the hunter-gathers. The second technological stage was the creation of the machine. A machine (a powered machine to be more precise) is a tool that substitutes the element of human physical effort and requires only to control the function. Machines became widespread with the industrial revolution, through windmills, a type of machine, are much older. Examples of these are cars, trains, computers and lights. Machines allow humans to tremendously exceed the limitations of their bodies. Putting a machine on the farm, a tractor has increased the food productivity at least tenfold over the technology of the plow and the horse. The third and the final stage of technological evolution is the automation. The automation is a machine that removes the element of human control with an automatic algorithm. Examples of machines that exhibit this characteristic are digital watches, automatic telephone, switches, pacemakers and computer programs. It is critical to understand that the three stages outline the introduction of the fundamental types of technology and so all three continue to be widely used today. A spear, a plow, a pen, a knife, a glove and an optical microscope are all examples of tools.

- Theoretical Implications:

The process of technological evolution culminates with the ability to achieve all the material values technologically possible and desirable by mental effort.

An economic implication of the above idea is that intellectual labour will become increasingly more important relative to physical labour. Contracts and agreements around information will become increasingly more common at the marketplace. Expansion and creation of new kinds of institutes that works with information such as universities, book stores, patent-trading companies etc. are considered an indication that a civilization is in technological evolution.

This highlights the importance underlining the debate over intellectual property conjunction with decentralized distribution systems such as today's internet. Where the price of information distribution is going towards zero with ever more efficient tools to distribute information is being invented. Growing amounts of information being distributed to an increasingly larger customer base as times goes by. With growing disintermediation in said markets and growing concerns over the protection of intellectual property rights, it is not clear what form of markets for information will take the evolution of the information age.

The Social Impact of Technology

There is no doubt that technological change brings about social change. The Industrial Revolution aw many people displaced from their land, to find work in crowded city factories. Serfdom was abolished and population shifted from villages to the cities. Strong family ties, self-sufficiency and the

right to occupy land were replaced with uncertain tenancy of land, dependency on trade and a weakening of the family unit. Economically, goods and money abounded and trade flourished. The merchant class profited from the wealth that was generated on the backs of the displaced population in urban workers. Children were sent to work in factories, in order for families to make enough money to live. The peasant class worked long hard hours in poor conditions with no security. The industrial revolution led to the alienation of the working class and although many union battles have since led to the adoption of better working conditions, the effects of industrial revolution remain. The family unit is even more vulnerable today with soaring divorce rates, high rates of teenage suicide, most of society are either heavily mortgaged to banks or paying high rents and no-one can be self- sufficient in a world governed by free trade.

Advances in technology, is generally not equitably shared within society. People with moneyhave more opportunity to acquire technology, which enables them to acquire more wealth. It is also important to remember that war has been and will continue to be the driving force for technology and innovation. Power and wealth are intrinsically tied together. Technology leads to a greater socio economic division. Labourers are viewed as commodities and expendable. Technology leads to alienation because it can create jobs that require no specialist knowledge.

Till date, since the industrial revolution we have seen technology used to the detriment of society. The right to occupy land has become a privilege that must be worked for and earned and now the battle is on to control all the world's food and textiles through genetically modified seeds and animals. The insidious part of genetically modified is that, there is no recall once it is released into the environment. The weed plants that will grow ten times faster than normal weed plants will destroy river systems, as their unfair genetically modified crops that are dependent on pesticides will contaminate organic, heritage seeds that have sustained people for thousands of years. Seeds will no longer be able to be harvested and re-planted but the farmer will have to buy new seed every year from genetically modified seed makers. This fight is more important that the fight over open source because it involves the right of people everywhere to have clean, safe food that has not been genetically altered. It is essential to mention that genetically modified is a tax on everyone because a patent will be on every seed and seeds are made to be sterile the following year. This is something to become angry about. The greedy corporations and individuals that want control over our food, water and land, do not care about the irreversible damage to the environment, people and animals they cause.

We have the right to eat tomatoes that are free of fish DNA, meat and milk that is free of human DNA, pigs that haven't been grown to harvest anthrax antibodies. They will never be able to prove the safety of Genetically Modified food and no long terms studies have been done. Nor will genetically solve the problem of soil erosion and polluted of rivers from artificial fertilizers and pesticides. Only a return to

responsible organic and biodynamic farming practices will solve these problems.[2]

The internet in its current form was developed as a free exchange of information, unregulated by any one government or owned by one person or company. In this raw form it was the playground of hackers and computer geeks, who challenged the status quo. It brings about a new era, the technological revolution. The free flow of information, has brought about technological advances at an unprecedented rate and has made many rich and brought companies who failed to adapt to a standstill.

How will the technological revolution impact on our society? If the industrial revolution is anything to go by, there will be winners and losers to technological revolution.

E-Commerce will affect the middle man and allow direct trade with consumers. Efficiency brings about lower prices for the consumer, but it is more accurate to argue that efficiency brings about greater wealth for shareholders, directors and owners. The intrinsic weave of social interactions of trade, can be disentangled and made into a horizontal supply chain. E- Commerce will create efficiencies that effectively remove the need for a long supply chain but at the expense of social relationships.

The effect of E-Commerce and the internet will impact on every society on the earth. Already, the barriers of trade between individuals in different countries are non-existent. Company contact details are searchable through powerful search engines and trade can commerce between two individuals who would otherwise never have met. The internet dissolves national boundaries and the consequences for cities that have developed as center of administration and trade will be disastrous, if they do not embrace the technological advances in communication and trade that the internet brings. While at the same time, free trade means fierce competition without the protection of award wages. People are reduced to consumers and suppliers.

Resisting the tide of technological change is impossible. Of course it is possible to do business without a website or email or mobile phone of a fax machine. People have been doing business well before any of these gadgets were invented. But business today is about competition and technology is about leverage. Technology can lead to alienation if it is not widely dispersed in society. The industrial age saw the concentration of technology in the hands of the rich and powerful, allowing them to dominate and subdue the population into harsh working conditions and the social impact of the internet and computers is only just beginning will it challenge the status quo or will it lead to greater population control?

Already technology like digital T.V. is being pushed in the guise of better quality but the benefits to those who own the systems is that they will be able to track what you watch, when you watch it, whether or not you switch off an ad. Knowledge is power and with access to tapping phone lines, reading e-mails, reading your credit cards statements, knowing by GPS where you are by tracking your mobile phone, it can be scary world, if all that knowledge and power were to be used to oppress and control.

[2] See http://www.cqs.com/50harm.htm and See http://www.seedsavers.net

On the upside, technology has made the developed world a richer place to the detriment of the environment. Technology has gone too far and there are more people counting beans than growing them.

Impact of Technology on Government

The legal system is dependent on local jurisdictions under common law. Historically, one has to remember that before the age of the internet, airplanes and telephones, the vast majority of business was done locally. Technology has rapidly changed the way people do business but people and governments have not adapted to change to that same pace especially in India.

What are the implications?

If we buy a product from a local supplier in your state and it turns out that the item is faulty, we can go back to the supplier to work out repair or replacement and if they don't help us, then complaint can be made in Consumer Dispute Redressal Commission. However if we buy a product outside jurisdiction, claim can be filed in another state, where the supplier is located.

We have a world which is governed by local laws and yet the businesses and individuals are now actively trading outside their local area. Governments are trying to make laws about content on the internet but have no jurisdiction to enforce those laws. This has created havens in small developing countries, that are happy to accept companies that want to run online gambling websites that may be outlawed in their jurisdiction or companies that wish to reduce their tax liabilities by opening up bank accounts in developing countries.

We see arising now a homogenizing of local laws on the issues like 'SPAM' and even sending an international letter from anywhere in the world involves the completion of almost identical forms. Governments are making agreements, in an attempt to be relevant in a world where people are able to trade more freely and where digital communication has enabled businesses to work, almost without physical boundaries.

THE EVOLUTION OF CYBER SPACE

INTERNET USAGE AND PENETRATION IN INDIA:

In India the internet usage and population penetration statistics has been on the rise continually over the last decade. Data available on internet projects that whereas in India in 1998 there were only 1,400,000 users of internet and internet penetration was 0.1% only, in 2010 internet users grew ten crore and internet penetration reached 8.5%.[3]

SIGNIFICANCE OF INFORMATION TECHNOLOGY

The role of information technology in today's e-world is remarkable. It has extended efficiency, cost-effectiveness and accelerated productivity at individual as well as the business or governmental level. Internet has truly become an internal facet of our lives. People communicate within their social circles through blogs and social networking sites such as Facebook, Orkut, and Twitter and also transact business across borders with much ease and speed through the use of internet. The information technology age has strengthened our law

[3]See www.internetworldstats.com

enforcement systems and led to establishment of E-Courts in India where matters are filed as well as heard using electronic means. . In the case of Central Electricity Regulatory Commission v. Hydroelectric Power Corporation [4], the Supreme Court of India held that court notices should also be sent by e-mail apart from registered A.D. in order to avoid delays and observed that such practice should be followed in all commercial litigation wherein urgent relief is sought in the Supreme Court.

NO GEPGRAPHICAL DIVIDE:

It is also amazing to see how internet has blurred the time and geographical divide. While operating a computer station we are connected to cyberspace and are able to seamlessly transact business across different jurisdictions on touch of screen. Moving a step further, in 'cloud computing' [5] a user may request for a service on the internet and receive these from any server in any part of the world without knowing its exact geo location akin to supply of electricity by a service provider. Substantial data is uploaded, downloaded, stored, streamed and retrieved through internet which may comprise of confidential and proprietary data or information of social, economic or political nature. This has led to a debate in protecting privacy and data in the cloud computing age and adoption of security parameters to benefit from the new technology.

DRAWBACKS OF INFORMATION TECHNOLOGY:

While there are many advantages of information technology, there is also a flip side. The growing proliferation of e-crimes in cyberspace such as cyber warfare, cyber terrorism, hacking, data thefts, invasion of privacy, phishing attacks, intellectual property infringements and identity thefts and other computer related frauds. The e-crimes often pose serious threats to national security, cause danger to life and property and may cause economic loss to entities and individuals apart from threat to one's privacy and freedom in cyberspace. There are growing instances of behavioural advertising, corporate espionage, data mining, employee surveillance and illegal use of web bugs and cookies which is also an affront to the right of privacy of individuals.

THE DIGITAL DIVIDE:

In many countries like India despite growing internet and mobile usage, there is still a digital divide that poses a clear challenge. The affordability, availability of technology, literacy and ready access to computers and mobile internet phones are important factors that decide penetration levels of Information Communication Technology (ICT). TheGovernmentof India has adopted several ICT and e- governance schemes in the country, including initiatives to spread internet connectivity among the masses. This initiative of the Government has been termed as 'Digital India.'[6]

[4] 2010 (10) SCC 280

[5] It is a web network service that enables virtual sharing of software, resources for storage and processing, or retrieval of data as a utility service. It is similar to electricity to electricity supply wherein end user does not know the origin and travel path of electricity supplied to a user.

[6] Digital India is the flagship Programme of the Government of India to digitally empower its people and India's economy. Its vision is three fold namely

VOLUME 6 ISSN 2456-9704

ORIGIN OF CYBERSPACE

The cyberspace means the virtual world created by mankind using computers and networking through which they interact and exchange information using multiple languages or communication protocols that are created by humans so that one computer can talk to another computer. Our internet is the same virtual space with no physical boundaries and powered with technological dynamism and speed. The expression 'Cyber Law' covers all case law and statutes, statutory regulations, codes, legal principles that state and its authorities legislate to govern acts of persons and entities while they perform acts on the internet or in connection with internet. The expression includes law that governs those entities that provide or facilitate the internet access or entities that use cyberspace for displaying information or e-commerce and entities that manufacture that sell hardware and software.

GROWTH OF INFORMATION TECHNOLOGY

creation of digital infrastructure, governance and services on demand and digital empowerment of citizens. It aims to leverage the common and support the ICT Infrastructure established by Government of India and revamp their existing e-governance services, inclusion additional state specific projects, adopting a decentralised implementation model. Public Private Partnerships are preferred wherever feasible and adoption of Unique ID would be promoted to facilitate identification, authentication and delivery of benefits. Digital India Programme has nine pillars. These are broadband highways, e-governance reforming government through technology, electronic manufacturing, universal access to mobile connectivity, E-Kranti electronic delivery of services, IT for jobs, Public Internet access programme, Information for all, early harvest programme.

MEANING AND SCOPE OF INFORMATION TECHNOLOGY

The 'information technology' can be defined as computers and computer networks, internet infrastructure and topography, software, websites and internet based communication technologies and its in-depth scientific knowledge that is used to upload, access, search, process, share, transmit, post, update information including textual and multimedia based images or other information. The term 'information technology' includes hardware, databases, programs and other internet related equipment used for storage, processing and transmission of information across computer network.

LEGALISSUES IN CYBERSPACE

Cyberspace is unlike the traditional offline world that has over a period of time developed settled legal principles that govern people's actions and rights over their property. The cyberspace is comparatively a fairly recent invention and jurisprudence in cyber law is still at a nascent stage is gradually evolving. While certain laws applicable in a conventional offline are being adapted to an online world. There are other different Legal Issues in Cyberspace.[7]

[7]Legal Issues in Cyberspace are:

- Applying existing Laws or making new laws?
  The issue presents an unending debate between creation of a specific law that would govern one's actions over the internet as a distinct from the offline world or simply adapting offline laws to the new virtual cyberspace. The dynamics of information technology requires special treatment due to its unique and inherent matrix and far reaching implications. Information technology Law requires special law to be developed.
- Contractual and Non-Contractual issues
  Many interesting and intriguing questions surface when one attempts to apply territory specific laws

to acts or omissions committed over internet. While internet law regulation is being developed and few cases have been developed and few cases have been decided with regard to internet yet there are many complicated legal issues that will have to be resolved with the passage of time.

- Legal Recognition to E- contracts and E-Signatures
  The approach of the courts in most jurisdictions is to apply principles of formation of contracts and applicability of jurisdiction to the e- world as these principles apply in a conventional setting. There is a general consensus that electronic signatures and electronic documents are legally valid and stand on an equal footing to handwritten signatures or paper based documents. The United Nations Commission on International Trade Law working group on Electronic Commission framed the model law on electronic commerce in 1996. The Model Law emphasizes on the principles of 'Functional Equivalence.' India in the year 2000, enacted its first law of information technology based on fundamental principles elucidated in UNCITRAL Model Law of E- commerce.
- Privacy and Data Protection
  Apart from contractual matters, several non-contractual issues arise under Tort Law which are often intertwined with jurisdictional issues. Other Legal issues which confront us on the internet include concerns over freedom of speech on the internet and privacy and data protection issues. Several countries have already introduced comprehensive laws to deal with UK Data Protection Act in 1998. In European Union (EU), the Data Protection Directive was passed in 1995 whereby EU laid strict guidelines on data collected from persons and its authorized use and related matters.
  In addition, intellectual property infringements are rampant on the internet due to the ease with which trademarks and copyrighted materials can be copied and distributed in cyberspace.
- Freedom of Speech
  The other non- contractual matters involve issues of protecting freedom of speech and privacy in the cyberspace. This may assume different dimensions and effects including posting of obscene information, defamation, hate speech and acts which threaten national security and public order. Protection of privacy and data is of vital significance in the online world. However, a delicate balancing of interests of both government and individuals is required for both national and public interest.

JURISDICTION IN BORDERLESS CYBERSPACE

Unlike the conventional world, territorial borders do not exist in the virtual world. The cyberspace is one single space devoid of national boundaries. We need to understand the key principles to determine jurisdiction in cross border online disputes between them. We need to understand the key aspects of internet law such as e-contracting, e-commerce, taxation amongst other legal aspects. We need to learn the meaning of jurisdiction.[8]

THREE PRE-REQUISITES OF JURISDICTION

For a judgement to be valid and enforceable, three pre-requisites need to be satisfied, namely, (1) the jurisdiction to prescribe[9], (2)

[8] 'Jurisdiction' means the power or authority of a court to adjudge a case. In case court lacks jurisdiction, its judgement has no force in law. Jurisdiction is mainly categorized into three types namely (1) subject matter jurisdiction, (2) personal jurisdiction, (3) pecuniary jurisdiction. All the three are required to be satisfied if a judgement delivered by a court is to have validity and enforceability. The term 'subject matter jurisdiction' means power of the court to hear and decide specific cases that can be categorized in a subject matter domain. The forum where a legal dispute is or a claim is filed, ought to have an authority to decide a matter pertaining to specific subject matter or domain. 'Personal Jurisdiction' is the authority of a court to hear and decide a case against a particular set of persons. 'Pecuniary Jurisdiction' refers to jurisdiction of a court based the amount of claim which is made in a proceeding.

[9] Jurisdiction to Prescribe- It means that the laws and regulations of country apply to a particular category of persons. The jurisdiction to prescribe is the power

the jurisdiction to adjudicate[10] and (3) the jurisdiction to enforce.[11] According to international law, a country's power to exercise jurisdiction over non-residents that may conduct business or have other interests in their country is largely limited. In many cases a non-residents that may transact online business and solicit business in a forum state where he does not reside. Many countries have evolved principles that apply in similar situations to determine jurisdiction involving cross border online activity.

JURISDICTIONAL THEORIES IN JURISDICTION TO PRESCRIBE

Whether a state has *jurisdiction to prescribe* is based on different theories. These are (1) Subjective Territoriality[12], (2) Objective Territoriality[13], (3) Nationality[14],

of a state and its privilege to apply its laws to persons, their activities or belongings or interests, status of persons and their interpersonal relationships and business entitlements in that state. In USA the Restatement of Foreign Relations law of the United Nations, 1987, explains when a country has jurisdiction to prescribe law, i.e. it will have jurisdiction to prescribe law with respect to-

- Conduct that wholly or in substantial part, takes place within its territory,
- The status of person or interests in things present or interests in things present within its territory,
- Conduct outside its territory that has or is intended to have specific substantial effect within its territory,
- The activities, interest, status, or relations of its nationals outside as well as within its territory,
- Certain conduct outside its territory by persons who are not its nationals outside as well as within its territory
- Certain conduct outside its territory by persons who are not its nationals that is directed against the security of the country or against a limited class of other national interests.

These principles are popularly known as territorial principles, nationality principles, the effect principles and the protective principles respectively.

[10]Jurisdiction to adjudicate- It means that a forum of adjudication has the power to decide a dispute concerning a person or a thing. To fulfil the jurisdiction to adjudicate, a country must have the jurisdiction to prescribe the law that it seeks to apply to decide the subject dispute. According to the precedents involving issue of determining jurisdiction over a non-resident defendant, a number of factors are considered by courts to decide if they hold jurisdiction to adjudicate the matter. The need of reasonableness is always a threshold requirement.

It is pertinent to note that if it is reasonable it does not necessarily imply that the forum state has also the jurisdiction to prescribe. In many cases there may be jurisdiction to prescribe, for instance in India, The Information Technology Act, 2000 (IT Act, 2000), Section 1(2) read with Section 75 wherein the act states that it applies to any offence or contravention committed outside India by any person apart from its application to the whole of India. According to Section 75 of IT Act, 2000, the Act applies to any offence or contravention committed outside India. This means that the act has prescriptive jurisdiction over non-residents who may commit an act that amounts to an offence outside India.

[11]Jurisdiction to Enforce- it means a state's power to direct a person to mandate compliance of its rules and regulations by various means including administrative or police action or judicial or non-judicial action. The jurisdiction to enforce will apply only if a state has the jurisdiction to prescribe. Very rarely a state may allow another state's law enforcement team to enforce their own state's laws within the jurisdiction of another state without due written consent of the state.

[12] The subjective territoriality means that if a particular act or conduct is committed within the boundaries of the regulating state then such state shall be entitled to lay down law that would govern such act or conduct.

[13] The objective territoriality finds its application where the act in question takes place in another territory. However, the effect of the activity, direct or indirect is substantially felt within the forum state. Commonly known as the "effects jurisdiction", this principle has emerged into a widely accepted test to determine jurisdiction in cyberspace.

(5) Protective Principles[15] and (6) Universal Interest Jurisdiction.[16]

INDIAN LAWS TO DETERMINE PERSONAL JURISDICTION

- Selection of Forum by Choice:
The parties to contract are free to decide the forum where they agree to decide their disputes. In case where there is conflict of jurisdiction, the choice of jurisdiction shall be made by the plaintiff based on convenience unless a law excludes such option of access or it would amount to abuse of process of court or against public policy. 'Public Policy' means not merely policy of a government but also includes matter which is for public interest and public good.
- The Code of Civil Procedure, 1908, Information Technology Act, 2000 and Jurisdiction:
Under the IT Act, 2000 there are no separate criminal courts to decide cybercrime matters and such cases are heard by criminal courts established to hear general criminal matters. In civil cases wherein compensation is claimed for any contraventions as provided in the IT Act, 2000, the Adjudicating Authority is empowered to grant compensation by virtue of Section 46 of the IT Act, 2000. Such cases involve, for instance where someone unauthorised deletes data of another person, introduces virus, or copies or extracts certain data amongst other acts mentioned in Section 43 of the said act. For seeking injunction orders, for instance in Trademark infringement matters, courts where plaintiff resides, or personally works for gain determines jurisdiction (Section 134 of Trademark Act, 1999) while Section 20 CPC also allows case to be filed where part of cause of action arises or where defendant carries on business. There are other relevant provisions of Civil Procedure Code.[17]

E-CONTRACTING

The formation of contract in cyberspace has intrigued legislators and academicians of several countries. The tradition rules of formation of contracts in the offline world are more or less settled. However, on the internet the same [principles may not find equal application.

FORMING AN E-CONTRACT THROUGH WEBSITE:

Whenever a company has an e-commerce based website it enters into contracts through various advertisements posted on their website which constitutes an 'invitation to treat.' While surfing on the internet, we often come across websites which are shopping sites, auction websites where several products are being advertised for sale originating from several manufactures. There are also manufactures who have dedicated websites consisting of

[14] The principle of nationality applies where the alleged offender is a national of the state, the laws of which have been violated by his acts. The forum state assumes jurisdiction based on nationality principles.

[15] The protective principle finds application where a country takes necessary action in a foreign state to secure its national integrity or interest.

[16] This jurisdiction is assumed by any state to prosecute an offender for acts which are known universally by International Law to be a heinous crime, i.e. hijacking, genocide, child pornography.

[17] Relevant provisions of CPC- The Code of Civil Procedure, 1908 prescribes pecuniary jurisdiction limiting the powers of the court to hear matters up to a particular pecuniary limit under Section 6. As per Section 16 of CPC, the jurisdiction in a case is also determined on the criteria of where the subject matter is situated.

advertisements, brochures and catalogues of various goods they manufacture. Each case has to be analysed on the basis of facts and circumstances. Nevertheless, the words used for the advertisements and the intended purpose of website form material consideration for the analysis. On the e-commerce websites a user is asked to register where he fills in his personal particulars and contract information.
Basically, ine-contract websites there are three types of contracts. These are Clickwrap, Browsewrap and Shrinkwrap contracts.

CLICKWRAP AGREEMENTS:
In the case of a 'Clickwrap Agreements'[18], the terms and conditions are mentioned on a website to which a user indicates his acceptance by clicking on the 'I agree' button on the screen. Sometimes in the place of 'I agree' button similar connotations indicating acceptance of user may be used. The clickwrap agreements are often used in downloading software and contain provisions to protect the intellectual propertycontained therein by restraining the licensee from selling the copy of his software. It also contains provisions that disallow any decompiling of the program for any purpose.

Browsewrap Agreements:
In a 'Browsewrap Agreements'[19], the terms are a part of the website content but, does not require to specifically grant his assent and mere browsing of website may constitute a user's consent. Generally, in all e-commerce websites the terms and conditions are prominently displayed on the website and at the earliest opportunity the attention of a user is drawn to read the same.

Shrinkwrap Agreement:
Shrinkwrap Agreements[20] have met with some criticisms by the courts and a court may not enforce a contract if it is of the view that such a contract is 'unconscionable at the time it was made.'

VALIDITY OF SHRINKWRAP, BROWSEWRAP AND CLICKWRAP AGREEMENTS:
Article 11 of the UNCITRAL Model Law on Electronic Commerce (1996) grants recognition to the validity and enforceability of Clickwrap Licenses. Similarly, under Section 10A of the Indian Information Technology Act, 2000 confers legal recognition to electronically formed contracts. Since there are no cases under all these three agreements, such contracts will be held valid and enforceable as long as contracts satisfy basic ingredients of formation and are not tainted with undue influence under Section 16 and opposed to public policy under Section 23 of the Indian Contract Act, 1872.

[18] An agreement formed by a confirmed acceptance online given a user by accepting the terms published on a website by clicking on the 'I agree' or similar button denoting his consent to formalize the agreement and abide by terms of use mentioned for a transaction or web service.

[19] Browsewrap terms do not require an express consent of the user and its terms are generally accessible through a hyperlink on the website. Merely by browsing a website if a user's consent is deemed, it forms a browsewrap agreement.

[20] An agreement formed with a customer wherein some terms of agreement are packed inside the package of a product such as software. Generally in the case of Shrinkwrap Agreements, if the product's sale and purchase terms are not acceptable to a user after he opens the package, the product can be returned within specified time window.

REQUIREMENT OF WRITING IN E-CONTRACTS:

In most jurisdictions, for a contract to be valid and enforceable, it is required to be in writing. A written contract grants reasonable certainty of its existence and is clearer as regards the terms agreed between parties. According to Model Law, whenever any information is required in writing, such requirement is satisfied by an electronic message if the information in data message is accessible and usable for a subsequent reference.

POSTAL RULE IN ONLINE CONTRACTS:

Under the conventional common law principles of contract law, a legally binding contract is formed when an offer is given its assent in the manner required by the terms of the offer. According to Common Law principles, an acceptance communicated through post is complete when the letter is posted or by telegram when it is handed. This is known as 'postal rule.' As per the 'postal rule' a contract is formed when a written acceptance has been posted.

UNITED NATIONS CONVENTION ON THE USE OF ELECTRONIC COMMUNICATION IN INTERNATIONAL CONTRACTS, 2005

The Convention was adopted by the General Assembly on 23rd November 2005 and deals with increasing 'legal certainty and commercial predictability where electronic communications are used in relation to international contracts. It lays down guidelines for determining a party's location on the internet, the time and place of dispatch and receipt of electronic messages, e-contracting through automated systems and parameters for functional equivalence between electronic records and paper based documents.

EUROPEAN UNION LEGISLATION ON E-CONTRACTS[21]

The EU has created many important laws to grant legal recognition to e-contracts and to facilitate e-commerce activity. Among the important directives are the Electronic Commerce Directive, Unfair Contract Terms Directive, E-Signature Directive, Time Share Directive, The Privacy Directive and Directive on Enforcement of Intellectual Property Rights.

INDIAN APPROACH TO E-CONTRACTS

The Information Technology Act, 2000 is enacted based on the UNCITRAL Model Law of E-Commerce. The IT Act, 2000 grants legal recognition to electronic records and states that the requirement in 'writing or type written or printed form' will be considered as fulfilled if the information is made available in an electronic form and accessible for use for a subsequent reference. There are many relevant provisions under IT Act, 2000.[22]

[21] See Karnika Seth, Computers, Internet and New Technology Laws, Second Edition 2016, page 89

[22] Relevant provisions are:

- Section11 of the IT Act, 2000 provides that an electronic record is attributed to the originator if it was sent by the originator himself or a person duly authorized by the originator or by an information system programmed by the originator to send the message automatically.
- Section 12 of the IT Act, 2000 elucidates Section 12 of the IT Act, 2000 elucidates that when the originator has not specified that an acknowledgement of receipt is required in a particular format or method, an acknowledgement can be given through any communication by the addressee 'automated or otherwise' or by the

ELECTRONIC COMMERCE

Use of computers and Information Technology to transact business by and between entities and individuals is termed as electronic commerce. Now a days, markets have been transformed to online shopping malls where Business to Consumer (B2C) and Business to Business (B2B) transactions materialize using payment gateways and online contracts. The accessibility and ease of using Information and Communication Technology (ICT) propelled internet based payment systems including net banking and mobile payments that has been a key factor in the growth of E-Commerce.

ADVANTAGES OF E-COMMERCE:[23]

E-Commerce has many advantages. Because internet is accessible, user friendly, cost effective and effective means of transacting business, its advantages have increased.

RESTRICTED ACTIVITIES IN E-COMMERCE:

Another issue that arises in the context of e-commerce is that different jurisdictions have different laws to regulate online activity. For instance, in India, any online gambling website is banned and any online money transfer services require permission from Reserve Bank of India to operate its business in India. In European Union (EU), online shops selling drugs is a regulated activity and in Germany online pharmacy is permitted. Many countries like India either prohibit or restrict websites selling Narcotic Drugs, hazardous chemicals, explosives, firearms, live animals, alcohol, gambling and pornography on the internet and even otherwise.

LINKING, FRAMING AND METATAGGING IN E-COMMERCE:

Another aspect of e-commerce is active advertising through linking[24] and framing[25].

conduct of the addressee that reasonably indicates to the sender of a message that the electronic record has been received.

- Section 13 of IT Act, 2000 regarding time and place of dispatch and receipt of electronic record, the dispatch of electronic record occurs when it enters a computer resource outside the control of the originator.

[23]Advantages of E-Commerce:

- Electronic commerce has revolutionised the methods of undertaking business in almost all the sectors of activity including education sector where most courses are now offered online through distance education.
- The global nature of cyberspace and with the ease of communication both traders and individuals benefit from cross border business opportunities are available online. A consumer has wide range of options to choose from and large amount of updated information at his disposal to arrive at a decision while purchasing goods and services online.
- Now, the domestic industry is able to procure raw materials from across borders. For instance, it is commonly known that in the tyre industry and chemical sector Indian importers sign e-contracts with Chinese suppliers to order raw materials.
- US entities have started to outsource office functions back into India. With this, significant cost reduction in the BPO, KPO, LPO sectors as vast amount of information can be easily processed and transmitted across borders at one-tenth cost.
- For a consumer it is far easier to conduct research on a topic, assess and analyse, an offer of goods and services online. For a consumer, e-commerce is a boon offering myriad choices of products and services across diverse markets and quick access to consumer reviews on consumer websites and blogs enabling easy comparison and decision making more convenient.

[24]It is a term used to describe practice of linking or connecting information on a webpage that is shown in highlighted text which contains link to another website to allow a user to efficiently browse required

In most jurisdictions courts have relied on national laws to decide any dispute that may arise involving linking and framing within their national frontiers. The general understanding is that a person who links to a website does not endorse its content. This principle is usually incorporated in its terms of use policy, privacy policy and disclaimers mentioned on the website. In the case of metatagging[26], keywords may infringe Trade Mark Law and constitute an unfair trade practice.

UNCITRAL MODEL LAW ON E-COMMERCE:

United Nations Commission on International Trade Law (UNICTRAL) adopted the Model Law on E-commerce in the year 1996. The Model Law aims to facilitate electronic commerce by overcoming legal hurdles in international trade through internet. The Model Law has been adopted as guiding text for enactment of India's IT Act, 2000 incorporating specific provisions on e-contracting and e-commerce. Model Law is explained through a guide of enactment. The Guide to Enactment explains that the Model Law adopts a functional 'equivalent approach' and declares that the paper based contracts are as legally valid as electronic documents. Model Law studies basic functions of paper based documents and provides adequate criteria for electronic records, which when adopted, will grant the same legal recognition to an electronic record as granted to a paper based document.

INDIA'S APPROACH TO E-COMMERCE:

The Indian IT Act, 2000 is based on the Model Law on Electronic Commerce adopted by United Nations Commission on International Trade Law. There are various provisions in IT Act, 2000 to facilitate e-commerce.[27]

ELECTRONIC SIGNATURES

With the introduction of internet and computers has introduced a dynamic change in the manner of forming contracts using 'bits and bytes' instead of ink and paper. The conventional 'ink and paper' model had its advantages that it can be proved easily, it has its own disadvantages that exchange of written documents will take more time and cost. At the same time there may be some authenticity in online transactions, problems like unauthorised interception, identity thefts, cheating by personation and anonymity in cyberspace. It is also easy to

information on the web. When it takes a user to a home page of another website, it is known as surface linking and if it takes a user to a page inside website, it is known as deep linking. Both require prior permission of the owner whose website is to be linked.

[25]On the internet framing takes place when a website uses its own frame but takes a reader to the content of another website which displaying the content of another in its own frame to create a false impression that the content belongs to the website of that frames. It is a form of copyright infringement.

[26]It means the use of keywords which are trademarks of the competitor used as hidden key words.

[27]Provisions to facilitate e-commerce are:

- Section 3 of IT Act, 2000 deals with authentication of electronic records.
- Section 4 of IT Act, 2000 grants legal recognition to electronic records.
- Section10A of IT Act, 2000 provides that contracts which are formed by electronic means shall not be unenforceable only on the ground that such electronic means were used to form the contract.
- Section 17 to Section 39 create the legal framework and infrastructure to support an efficient e-commerce regime.

tamper electronic documents without easy detection. To combat these challenges, use of sophisticated techno-legal solutions to fulfil the functional equivalent approach.

SIGNIFICANCE OF ELECTRONIC SIGNATURES

E-commerce activity is now largely facilitated by the use of electronic signatures in online transactions. It is now common practice to use digital signatures to sign and file documents to incorporate company in India with the Registrar of companies. In some government offices in India, a digital sign on an electronic digipad is used for authentication and identification. The risk of anonymity, identity theft, criminal impersonation, consumption of time and cost and logistic problems are some of the reasons why electronic signatures are important to secure internet transactions.

MODES OF ELECTRONIC SIGNATURES:

The most important mode of electronic signature is PKI.[28] There are many other important modes of electronic signatures.[29]

UNICTRAL MODEL LAW ON ELECTRONIC SIGNATURES, 2001:

The Model Law of Electronic Signatures adopts a technological neutral approach and does not approve or specify any particular form of electronic signature for authentication purposes. The Model Law also explains the 'rules of conduct' to indicate the obligations of the signer, the recipient and the role of a Trusted Third Party (means certifying authorities that grant electronic signatures to a person).[30] The Model Law on Electronic Signatures defines an 'electronic signature' as data in electronic form affixed to a data message that identifies and verifies the signer with recording a data message and describes his consent to the content in such data

[28] One of the most important and widely accepted methods of signing electronic documents is the technique known as Public Key Cryptography (PKI) or Public Key Infrastructure Model.' The digital signature affected by the use of the PKI method is one of the forms of affixing electronic signatures. Asymmetric Cryptography or PKI is based on two keys, public and private, which are mathematically linked with each other. A signer signs with the private key and a recipient decrypts the message with public key which assures reliability and verifies source of origin of message. On encryption, hash value matches with decrypted message hash value which will remain the same if the message has reached the recipient untampered. Another form of electronic signature is symmetric key cryptography which consists of key pair that is mathematically identical and is used by both signer and the recipient to encrypt or decrypt a message. It has greater chances of being compromised and for this reason asymmetric cryptography is preferred over symmetric cryptography. Electronic signatures can be used for other methods of verification such as use of biometric device involving handwritten signatures where a signer signs manually using a unique pen like device on a digipad or directly on a computer screen. This signature will be converted and stored in electronic form on a computer and attach to a data message for authentication.

[29] Other methods of electronic signatures include retina scanning, iris patterns, fingerprinting that records an individual's specific print or quality and measurement as identity proof of authentication. Furthermore, personal identification number (PIN) such as internet password or I-pin or password authentication, for example through input of alphanumeric digits is used to access one's e-mail account or clicking the 'OK' or 'I Agree' button to enter into an e-contract.

[30] See https://www.unictral.org/pdf/english/texts/electom/ml-elecsig-e.pdf

message.[31] The Model Law envisages three functions of electronic signatures namely, creation and reliance on an electronic signature and certification by a certifying authority. More than three entities could be involved when an electronic signature is affixed. Sometimes two of its functions could be fulfilled by a single party in case where the relying party also plays the role of certifying authority.

INDIA'S APPROACH TO ELECTRONIC SIGNATURES UNDER INFORMATION TECHNOLOGY ACT, 2000:

The IT Act, 2000 is enshrined with the provisions for electronic signatures.[32]

CRYPTOGRAPHY:

Cryptography [33] is of two kinds: (1) Symmetric Cryptography [34] and (2) Asymmetric Cryptography[35]. Encryption[36] is achieved by using cryptographic algorithms to convert a plain message into an encrypted form.

Public Key and Private Key:

In digital signature technology, the private key compliments its corresponding public key. The public key is used by the recipient of a message to verify digital signatures and the private key is required to be kept confidential by the signer. The private key can be stored on a smart card or to be contained in a PIN or in biometric device. While public key is made accessible to the public and usually published on a Public Authorities website, the private key is kept secret. The keys are based on mathematical algorithms and often use the prime numbers which are multiplied together to produce a hash number. It is impossible to derive a private key if a public key is known to individual. This feature ensures high security, authentication and integrity and ensuring non-repudiation of data messages.

[31] See Article 2 (1) of Model Law of Electronic Signatures

[32] Provisions for Electronic Signatures under IT Act, 2000 are:

- Section 3A defines requirements of electronic signature.
- Section 3A explains ingredients of electronic signatures.
- Section 3A sub-clause 2 provides that the signature should exclusively linked to the signatory and no other person and the 'Signature Creation Data' or 'Authentication Data', at the time of signing should be under exclusive control of the signatory or authenticator, any tampering of electronic signature or any change in information after being electronically signed should be detectable.
- Section 16 provides for security procedures and practices that are used to create 'secure electronic signatures' which bear a favourable presumption in law of its authenticity under evidence law.

[33] The digital signatures are based on encryption and decryption mechanism that ensure integrity and confidentiality of information that two parties may exchange on the internet. It is known to have its origins around 2000 B.C. In Egypt Hieroglyphics used cryptography to write on the tombs of their ancestral rulers.

[34] It involves a unique single secret key for both encrypting and decrypting a message.

[35] In the case of asymmetric cryptography, encryption and decryption involves a unique key pair namely Public Key and Private Key. The Public Key is used to retrieve a message and the Private Key is used to sign the same. In Asymmetric Cryptography, a Private Key is mathematically linked to a Public Key.

[36] This is a readable mechanism that converts a readable data into a humanly unintelligible form. This technique is used in digital signatures to encrypt data and is also used by banks to create secure payment gateways and in e-commerce websites. PKI (Public Key Infrastructure) technology uses this method for executing 'digital signatures". For decoding encrypted information into a human intelligible form decryption mechanism is not used. In a PKI, private key which is unique and confidential to the subscriber is used to encrypt the message and public key is used to decrypt it.

THE PROCESS OF CREATING DIGITAL SIGNATURE:

When the content is to be transmitted as a data message is selected by a sender, a 'Hash Function'[37] in the signer's software calculates a mathematical algorithm based hash result. This hash result will alter if a minor change is made to the data message. The signer's software converts the hash result into a digital signature by using private key of the signer. The digital signature is unique to the data message signed and the private key which is used for signing the data message. The digital signature attaches to the data message and is transmitted along with the message. There is a verification process of digital signature and should meet two conditions.[38]

ELECTRONIC MONEY

E-Money means prepaid money that is stored in an electronic format and used to pay for goods and services online. It includes prepaid online account, smart cards, e-wallets, and bitcoins, amongst other e-payment mechanisms.

ADVANTAGES AND DISADVANTAGES OF E-MONEY:

E-money has various advantages apart from low cost.[39] Besides this there are many other disadvantages of E-money.[40]

DIFFERENT FORMS OF E-MONEY:

[37]It is a mathematical process based on algorithms which is used to create and verify a digital signature. The use of 'Hash Function' compresses a data message into a 'message digest' of the message which is shown in the form of a hash result much smaller than the original message. In case there is any change or alteration in a message, a different hash result will be created whenever the same 'Hash Function' is utilized.

[38]The two conditions are:

- The signer's private key was used to sign the message. This will be confirmed if the signer's public key was used to verify the signature as the public key will verify the digital signature which was created with the signer's private key.
- The message was unaltered. This will be the case if the hash result calculated by the verifier matches with the hash result derived from digital signature when verifying the message.

[39]Advantages of e-money:

- The reduced overhead costs and processing delays are its prime benefits.
- Electronic Money can be transferred across without much convenience. It also brings transparency in payment transactions and payment systems like CC Avenue and PayTM. These systems grant certainty in the receipt of money.
- Digital money renders accounting of money and its storage fairly easy to manage. Use of Trust Seal and Secure Socket Layer, cryptography and authorized payment gateway such as CC Avenue offers great security to online transactions. These factors have stimulated increase in the e-commerce activity.
- Use of smart cards or e-money is not considered appropriate for high value transactions and credit cards and debit cards play a significant role in high-value transactions as these have been fairly more secure payment methods.

[40]Disadvantages of e-money:

- A rise in plastic money frauds due to skimming or cloning has led to introduction of new chip based encrypted cards that also bear magnetic strip to offer added security protection.
- Bitcoin is a form of electronic money where transactions are verified by network nodes or computers and recorded in a public distributed ledger called a block chain. It lacks centralised repository and is decentralised system. It is misused by criminals, particularly for darknet markets wherein their identity is camouflaged of spoofed by software and technical tools to commit crimes have caught the attention of law enforcement.

The payment of cash online involves different types of payment systems, including 'virtual money', 'the electronic wallet' and 'the virtual wallet.' Centralised systems such as PayTM, BHIM, web money sell electronic money to users through their centralized e-money infrastructure. Examples of decentralised electronic money are Monero which is an open source crypto currency which is secure and decentralized and Bitcoin and Ripple monetary systems which is a real time gross settlement system, currency exchange and remittance network by ripple. The third category of e-money is offline anonymous system and an example of the same is Digicash that does not trace one's identity. Electronic wallets utilize the Smart Card Technology which enables it to store the information about the card holders funds which are transferred from his account.

Similarly, E-Cheque is an analogous model of payment to the traditional cheque in the offline world. In this for example a customer sends payment to the merchant. The merchant presents e-cheque to the issuing organisation to receive payment. The details of the cheque are transferred electronically through electronic interbank compensation system and the fund is transferred similar to the processing of paper cheque.

PROTECTING PRIVACY AND DATA ON INTERNET

The right to 'privacy' can be defined as the right of a person to enjoy his own presence by himself and decide his boundaries of physical, mental and emotional interactions with other persons.

THREAT TO PRIVACY ON INTERNET:

The internet is a unique medium of exchange of information that contains vast information comprising of data which is stored and uploaded or downloaded. As more and more internet users surf the internet and post their personal information online, has led to scams of personal data. The virtual world has left no information private. Data thefts, corporate espionage, identity thefts and other crimes including defamation; kidnapping and murder have become a common phenomenon.

REQUIREMENTS OF PRIVACY POLICY AND TERMS OF USE OF A WEBSITE:

On internet sensitive personal information is gathered by credit rating agencies, payment gateways, employers, income tax department, service providers and by individuals. Any information that is posted on the website is no more private. For privacy policy, a user is often asked to provide personal information in order to register or create a new account to avail services from a website. This is done in order to check whether the person registering is fake or not.

INDIAN LEGAL FRAMEWORK FOR DATA PROTECTION AND PRIVACY:

Privacy protects different aspects of private interest including private interest protecting information that protects disclosure or misuse of sensitive personal information and 'autonomy interest' which includes discretion to make personal decisions and conduct activities in seclusion. Article 21 of the Constitution of India includes the provision of 'Right to Privacy.'

PRIVACY PROTECTION UNDER INFORMATION TECHNOLOGY ACT, 2000:

The Information Technology Act, 2000 is enshrined with many provisions for the protection of privacy on internet.[41]

CYBER CRIMES

MEANING AND AMBIT OF CYBER CRIME

In many 'Cyber Crimes'[42], the conventional crimes are committed through the use of internet or computer such as online defamation, cheating by personation, black mailing, fraud and criminal intimidation. Cybercrimes include crimes which are committed through use of computers or where a computer or computer network is the target of the crime. This category includes destruction of records, data theft and system hijacking amongst other crimes.

DIFFERENT KINDS OF CYBER CRIME:

Financial frauds are prevalent in the cyberspace due to technical loopholes and anonymity that exists in cyberspace. The following categories of cybercrimes are committed to make financial gains.

1. PHISHING

Phishing[43] is conducted through fax messages or other forms of instant communications like text messaging service. It is also termed as carding and spoofing. There are 'Hybrids of Phishing.'[44] Most Phishing attacks involve addressing the members without the original name and simply mentioning 'Dear Valued Customer', it may contain deceptive links which lead a victim to a fake website that may use a deceptively similar website address as an authentic service provides. Special training

[41]Privacy provisions under IT Act, 2000 are:

- Section 66E explains about violation of privacy.
- Section 67 provides punishment for publishing or transmitting obscene material in electronic form.
- Section 67A provides for punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form.
- Section 67B provides for punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.
- Section 69 confers power to issue directions fort interception or monitoring or decryption of any information through any computer resource.
- Section 69A prescribes power to issue directions for blocking for public access of any information through any computer resource.
- Section 69 B empowers the central government to authorise to monitor and collect traffic data or information through any computer resource for cyber security.
- Section 72 prohibits disclosure of information received by a person in his official capacity. This section imposes penalty for breach of confidentiality and privacy.

[42]A criminal act committed by making computer as a method or means of a crime to cause damage to persons and property is a cybercrime. When persons conspire to spread terror attacks, it amounts to cyber terrorism, if a person threatens to wage war over internet through writing against government, it is cyber war.

[43]The term is derived from the word 'fishing.' It is a form of financial crime or e-crime where a cyber-criminal disguises his true identity and sends out spam which appears like an authentic message, for instance a communication from a bank to authenticate one's net banking user name and password. These are fake messages that are sent to defraud the gullible netizens whose sensitive information such as credit card details may be stolen through phishing attack carried out by e-mail, such as credit card details, passwords from the users on the pretext of seeking authentication of a company's record.

[44]When phishing is conducted through mobile via SMS, it is termed as 'smishing' and if by telecalling, it is known as 'Vishing.'

workshops are being provided by service providers and other law enforcement agencies to spread awareness among the customers to detect phishing e-mails and encourage use of special software and spam filters to safeguard customers.

2. SKIMMING
   Skimming[45] is another form of cybercrime. It is necessary to take precautions against skimming.[46]
3. SPOOFING
   Spoofing[47] is a crime where a person on the internet disguises his identity. Sections 66D and Section66E of Information Technology Act, 2000 prescribes punishments for identity thefts and cheating by personation with a maximum term of three years of imprisonment and fine upto one lakh rupees.
4. Cyber stalking
   Cyber stalking[48] is a criminal offence in most jurisdictions including India. It is coupled with criminal intimidation, blackmail or extortion and puts the victim to threat to life or property and causes emotional harassment to the victim.
5. CYBERSQUATTING
   Cybersquatting[49], in India domain names have been conferred with the same protection as it is given to a trademark. A cyber squatter is liable to be restrained from using domain name in any manner and is required to transfer the domain name to the rightful owner, pay damages for trademark infringement apart from rendering account of profits.
6. CYBER TERRORISM
   'Cyber terrorism'[50], the attacks may cause physical or virtual violence which cause direct damage to nation's people and property or results in riots. The acts of cyber terrorism include damage to the protected critical computer systems that contain sensitive information of national interest, plane hijacking and crashes, automated bomb explosions and damage to any public utility services which are managed by the use of computer systems.
7. HATE SPEECH

[45] It is a form of cybercrime or fraud where a person steals the credit card number of a person by use of a copying machine called 'skimmer' when a credit card is swiped into a skimmer by a criminal secretly without detection by rightful owner such as at petrol station for example, it reads all magnetic data contained therein that can be used to clone the cards to commit unauthorized credit card transactions.

[46] Banks have adopted fire walls to protect their computer servers and data. Sophisticated software is used to conduct electronic banking and use of digital signatures for authentication process in order to maintain confidentiality and privacy of personal information.

[47] It means concealment on an electronic network such as internet protocol, spoofing using technical software such as Hide IP or identity spoofing through impersonation or webpage spoofing by creating by creating a deceptively similar webpage. Spoofing attacks can be curtailed by the use of firewalls that check and verify the origin and recipient of electronic message.

[48] The use of internet and its services such as blog, e-mail or chat services to harass, intimate, defame and stalk a person, threatening or causing mental agony ort injury to a person.

[49] It is used to denote an illegal act whereby a person intentionally books a domain name deceptively similar to the trademarks of its rightful owner and later offers the owner the domain name for purchase at a hefty amount.

[50] It means use of computers, computer networks, internet by criminals such as terrorists to spread error and crime that threatens the integrity, sovereignty, defence systems and public safety of a nation.

Under 'Hate Speech'[51], section 66A of IT Act, 2000 has been struck unconstitutional by the Supreme Court of India in the case of 'Shreya Singhal v. Union of India.'[52]

CYBER CRIMES UNDER INFORMATION TECHNOLOGY ACT, 2000:

The Indian Information Act, 2000 is enshrined with provisions related to cybercrimes.[53]

ELECTRONIC EVIDENCE

Electronic Evidence provisions under Information Technology Act, 2000. [54] Besides this, section 88A, section 85A, section 85B and section 85C of Indian Evidence Act, 1872 are relevant provisions.

EMERGING NEW ISSUES ON INTERNET

These include 'Behavioral Advertising'[55], 'Blogging'[56],'Cloud Computing'[57],'Unique Identification Number.'[58]

[51]It means writing posts on the internet which are aimed at defaming, intimidating or inciting violence or riots written against an individual or a specific group of individuals with a bias towards gender, religion, nationality, disability, sect, creed, region, social or political views, class, profession or physical attributes. It includes any oral communications apart from written matter on the internet.

[52]AIR 2015 SC 1523

[53]Provisions for cybercrimes under IT Act, 2000:

- Section 43 of the IT Act, 2000 provides penalty and compensation for damage to computer, computer system etc.
- Section 66 deals with computer related offences.
- Section 67 provides for punishment for publishing or transmitting obscene material in electronic form.
- Section 67A imposes punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.
- Section 67B provides for punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form
- Section 67C relates to preservation and retention of information by intermediaries.
- Section 68 provides for power to give directions.
- Section 69 provides power to issue directions for interception or monitoring or decryption of any information through computer resource.
- Section 69A provides for power to issue directions for blocking for public access of any information through any computer resource.
- Section 69B deals with the power to authorise to monitor and collect traffic data or information through any computer resource for cyber security.
- Section 70 provides for protected system.
- Section 70A deals with National Nodal Agency.
- Section 70Bprovides that the Central Government by the notification in the official gazette for Indian Computer Emergency Response Team to serve as national agency for incident response.
- Section 71 provides for penalty for compensation.
- Section 72 provides penalty for breach of confidentiality and privacy.
- Section 72A punishment for disclosure of information in breach of lawful contract.
- Section 73 imposes penalty for publishing [Electronic Signature] Certificate false in certain particulars.
- Section 74 provides for publication for fraudulent purpose.

[54]Provisions for electronic evidence under IT Act, 2000 are:

- Section 4 explains legal recognition of electronic records.
- Section 5 explains legal recognition to electronic signatures.
- Section 7 provides for retention of electronic records.
- Section 7A provides for audit of documents in electronic form.

[55]It means marketing or advertising practices and technologies adopted by E- Commerce entities on the internet based on behavioural patterns, browsing preferences, search queries of internet users who visit their websites.

[56]It is a web page maintained by a person who is the administrator and creator of the blog who regularly

CONCEPT OF ONLINE DISPUTE RESOLUTION

Online Dispute Resolution can serve as an efficient means of dispute resolution in cyberspace. It is a common belief that ODR may initially succeed in resolving small claims related disputes as opposed to the high stake matters a parties invariably prefer to enter into arbitration and present oral arguments in physical hearings in high stake cases. For ODR system to prove more practicable and feasible than litigation to a party, it needs to offer greater accessibility to technology, infrastructure, affordability, and convenience of use, flexibility, transparency apart from adequate security, impartiality, expertise and legal enforcement mechanisms. Therefore, propagation of ODR practices will involve spreading awareness, public-private partnership, IT training and education, developing an internationally accepted body of core principles and substantive and procedural law for ODR practices.

AUTHORS VIEW POINTS

According to me I have completed the task of conceptual analyses in the best possible way I could. The digital revolution has ushered a new millennium of increase in the use of computers and internet. With these there is a need for legislative framework. I have written the paper in such a way so that I am able to explain what technology can do for the mankind and what is the legal framework to protect the mankind. One thing we should all keep in mind is that with the pace in technology, ethical considerations should be kept in mind. This means the use of technology should be for the benefit of the people and not to exploit them. Analyses of legal methodology on computers and internet has been an invigorating experience of mine.

CONCLUSION

Technology has allowed man to move from manual labour of the fields to cities and machines. It has led to urbanisation and people have migrated to cities improved services and job opportunities. With the invention of computers till now the activity on the system has increased to an utmost extent. The law on computers and internet is based on UNCITRAL Model Law. This means, the states of the world have enacted legislation in accordance to it. But still, in developed countries the use of technology is much more than developing and under-developed ones. The crimes in the developed countries are also high. Therefore, developed countries should take stringent steps to control crimes on internet and this will automatically help developed and under-developed countries to overcome the challenges.

*****

posts its views on any topic that forms subject matter on the blog.

[57] It is a web network service that enables virtual sharing of software, resources for storage and processing or retrieval of data as a utility service.

[58] It is a twelve digit unique number which the Unique Identification Authority of India. Issues to all residents in India. The UID card bears the identification number that is stored in a centralized database and linked to biometrical information of a person such as fingerprint of all ten fingers and iris of each individual.