**International Journal of Academic Research and Development**
**ISSN: 2455-4197, Impact Factor: RJIF 5.22**
**www.academicsjournal.com**
**Volume 2; Issue 4; July 2017; Page No. 53-65**

# Offence under information technology act 2000

**Smariti**

LL.M., Net BPS Government Medical College Sonepat, Haryana, India

## Introduction

### Offence: Tampering with computer source Documents

### Computer Programming

Programming in a way of sending of instruction to the computer. These instruction are relayed to the computer by using programming languages. The programming this is a complex process of building blocks of Information system. It involves five steps to create individual programmes.

(a) Need analysis
(b) System design
(c) Development
(d) Implementation
(e) Maintenance

These five steps represent life cycle of the programme [1]. It all begins with identification and understanding of a need or a problem of the end users. It is followed by the design phase to articulate the logical steps in solving the proposed problems. Using techniques like flow charts, circles and massage pipes and pseudo codes the next step (development) involves writing the instructions to the computer, called source code, as well as testing those statements after they are writer. It is the most important time consuming phase of the entire 'life cycle' as it includes writing code, compiling correcting and we writing. Once, the programme is tested successfully without 'syntax and 'logical' errors it is installed on the hardware for use the work of the programmer continues as, the installed programme may require fixing of new errors (bugs), addition or modification of certain functionalities (maintenance).

The computer programme whether writer in machining language, assembly language or high level language is known as the source code. When the source code is translated by an assembler or a compiler into machine language it is known as subject code. In case where the programme is writer in machine language only, the programmes source code and object code are the same. The end user does not generally have access to the source code and as there are difficulties regarding retranslation, it is not possible to reconstruct to source code from the object code unless a decompilation programme is used to retrieve the original high-level language source code.

Source code represents the proprietary any intellect of a programmer. The information Technology Act, 2000 protect this proprietary intellect in the form of computer source code.

### S/65 Tampering with computer source documents

The wording of aforesaid section tends to create the nation of 'Property' while outlining the necessary ingredients related to the tampering with computer source documents. It protects the entire 'life cycle' if computer programmes as outlined in the concept note.

(a) Knowledg4e or intention to conceal, destroy or alter any source code used for a computer, computer programme, computer systems or computer network.
(b) Its misappropriation or conversion to one's own use, or use in violation of a legal direction or of any legal contract. The Explanation make the meaning of computer source code quite comprehensive as it include the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

The terms "computer source code" as defined in the Act incorporates the entire gamut of programming process. It includes computer commands programming code design prototypes, flow chart/ diagrams, technical documentation, design and layout of the necessary. Hardware, programme-testing details etc. Furthermore, it is important to know that the Act makes no motion whether the source code exists in tangible or intangible form. The Act accepts the computer source code in both the tangible and intangible form.

A source code is a computer programme written in any of several programming language employed by computer programmes. An object code is the version of a programme in which the source code language is converted or translated into the machine language of the computer with which it is to be used [2].

### Offence: Hacking with computer systems.

### The Hackers

The word 'hacking' has been much used and abused in the information technology lexicon. In its original technological sense, the word hacker coined at MIT in the 1960s. Simply con not a computer virtuoso. That's still the warning enshrined in the latest edition of the new hackers dictionary which defines such a person as someone 'who enjoys' exploring the details of programmable systems and how to stretch their capabilities one who programmes enthusiastically ever, obsessively.

In the last 40 years the hacking activity has seen many developments from purely a technology savvy art form it is now akin to a cyber-criminal activity. There were "True" hackers of 1950s and 60s who experimented with the capabilities of the large mainframe computers and

then there were "Hardware" makers of the 10s who played a key role in the personal computing revolution. The eighties saw the coming the age of "gave hackers". These were the creators of popular gamming. Software application for the hardware developed by the previous generation.

The early 90s saw the emergence of Hackers and crackers. The former identified itself with ethical hacking and the latter with unethical hacking. Computer hacking is the accessing of a computer systems without the express or implied permission of the owner of that computer system. Hacking is and international and coordinated activity. It is a pre-planned process, where first a target is identified; it is security features are studied, tools are developed to going unauthorized access and impair the normal functioning of a computer or computer systems. Examples of hacking activity way include.

1. Unauthorized input or alteration of input
2. Destruction/Supression/misappropriation of output from a computer process.
3. Alteration of computerized data.
4. Alteration or misuse of programs.

**Hacking: Authorized Access/Unauthorized access**

It all starts with gaining access to any computer resource. Mere access to any computer resource will not constitute an offence of hacking.

In DPP v. Bignell where two police officers were Charged for using the Police national computer to gain access to details of motor cars which they wanted for private purposes. They were charged with unauthorised access to computer material. Their appeal was allowed by the crown court and later confirmed by the Q B Divisional Court. It observed that the police officers were entitled to access such computer info. As part of their normal duties [3].

The access could be either authorised or unauthorised which may further lid to destruction or modification of inf. residing in the computer resource. Thus we way have situation

a) were 'authorised access' has lid to 'unauthorised modification' and
b) were 'unauthorised' access' has lid to 'unauthorised modification' 'Authorised Access' leading to 'unauthorised modification' is a 'post access' activity & any person or for that matter even all employee who has exceeded. His terms access right by subsequently indulging in all unauthorised modification of any given computer resource is liable under the aforesaid section S/66 But the case of "unauthorised access' leading to 'unauthorised modification' is slightly different. It involves both 'pre-access' and 'post-access' activities. Authorized or unauthorized access leading to unauthorized modification is one of the many critical essentials of hacking. The other essentials have been further elaborated by way of the explanation to the section 66 to distinguish hacking from other contraventions or offence U/ the Act.

**S/66 Hacking with computer system**

The aforesaid section defines hacking activity in a comprehensive manner. It takes hacking activity exclusively associated with the computer resource the essentials of hacking are

(a) Whoever
(b) Intention or knowledge
(c) Causing wrongful loss or damage to the public or any person
(d) Destroying or altering any info. residing in a computer resource or diminishes its value or utility of affects it injuriously by any means. Hacking would mean destruction or alteration of any information residing in a computer resource i.e. destruction or alteration of tangible or intangible assets of a computer resource one significant aspect is that the intangible asset will always be part of tangible assets for e.g. optical storage devices unlike CR—R, CD-RW, DVD – R, DVD-RW, represent tangible assets but may contain intangible assets in tell from of 'optical impulses'.

Interpreting the S/22 of IPC, the def. of "moveable property" is restricted to corporal property. It is property, which manifest itself physically. Apply this standard to a computer resource, one way find computer, computer system, computer work, computer hardware or any form of unmovable storage medium which includes magnetic or optical storage media, punched cards punched tapes fall in the category of "moveable property.

It was also cover image computer system computer network installations and server forms as they could be skewered farm the earth or laud to which they never attached and capable of being the subject of theft.

In Cox v. Riley [4] the question before court was whether unauthorized deletion or modification of computer programme embedded in a plastic circuit card that had been damaged but the programme the physical state of card remained unchanged and since the programme was intangible it could not be construed as 'property' within the meaning of S/10(1) of the Criminal Damage Act, 1971

In R v. Whiteley [5] The accused gained unauthorized access to joint Academic network and deleted added files. Changed passwords to deny access to the authorized users. Again the defence argument was that no criminal damage has been done to the 'properly' as defined under the 'Criminal Damage Act, 1971.

While deliberating upon such cases, one must not disregard the fact that proving destruction or alteration of data attached to an identifiable tangible property would not only be highly technical but may also bring all undesirable degree of uncertainty in the operation of law.

The perspective of the aforesaid section is not to nearly protect the information residing in a computer resource but to protect the integrity and security of computer resource from attack by unauthorised person seeking to enter such resources whatever may be their intention or motive. Under the Act, Hacking has been made a cognizable and non – bailable offence and is punishable with imprisonment upto three years or with fine which may extend upto two lakh rupees or both.

**Hacking: 5/43 V. S/66 of the Act**

As it has been argued earlier that there exist a thin line of demarcation between the provision of S/43 and S/66 of the Act. Whether it is about unauthorized access, unauthorized downloading, copying or extracting, introducing computer contaminant or computer virus, causing damage to computer data base or any other programmes, causing denial of access, providing any assistance to any person to facilitate access or availing any assistance to any person to facilitate access or availing of services on A/C of another person U/S – 43 of the Act, shades of S/66 can be seen.

The question is how to distinguish whether cyber crime falls under S/43 or S/66 of the Act. For a cyber crime to fall U/S 66, one must observe whether criminal intent was present or not criminal Intention simply means the purpose or design of doing an act forbidden by the criminal law without just cause or excuse. An act is intentional if it exists in idea before it exists in fact the idea realizing itself in the fact because of the desire by which if is accompanied. The criminal intent in hacking manifests itself in terms of causing wrongful loss or damage, destroying or altering any information residing in a computer resource or diminishing it value or utility or affects it injuriously by any means.

For e.g. a person causing a computer virus to enter into circulation is intentionally trying to impair the operation of a computer or any programme or date. The originator (or any other party who deliberately causes the dissemination of the virus) will be held responsible for the modification (impairment) of any computer, which is infected ever though he may not be responsible for the infection of any particular machine. Prima facie, the said person could reasonably be tried U/S – 43(C) or S/66 of the Act. Here in order to distinguish applicability of the section, one may have to look into the circumstances and accompanying events to the reconstruct the 'Chain of events' leading to circulation of computer virus. If the 'chain of events' points out a premediated, well-planned activity then it underling the presence of criminal intent to cause wrongful loss or damage and the S/ applicable would be S/06 of the Act. Any absence of criminal intent' would still make it punishable U/S-43 (C) of the Act

**Hacking and the Indian penal code**

Terms of hacking as defined under the Act seem somewhat similar to 'Mischief' as U/S – 425 of Indian penal code, 1860.

- Hocking U/ Information Technology Act, 2000
  Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroy or alters any information residing a computer resource or diminishes it value or utility or affects it inguriously by any means commits hacking.
- Mischief U/ Indian Penal Code, 1860
  Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person cause the destruction of any property or in the situation there of as destroy or diminishes its value or utility or affects it inguriously commits mischief. Thus hacking signifies mischief with the computer resource. It is the mischief regarding destruction or alteration of any information residing in a computer resource. And, it is mischief (hacking) with computer system i.e. using on computer to back into another computer. To brand any computer misuse us hacking would not only be fallacious but also against the spirit of the S/66 of the Act. It is important that fulfilment of all the ingredients as given in the aforesaid section are a must before an accused could be pronounced guilty of the offence.

**Offence: Publishing of obscene information in electronic force**

"If the depraved begins to see in these things more there what an average person would, in much the same way, as it is wrongly said, a Frenchman sees a woman's legs in everything, it can't be helped"

K.A. Abbas v. Union of India [6]

The issue of obscenity has always been one as it involves other related issues like decency and morality. This difficult to judge obscenity in isolation using straitjacket principles. It needs a wider perspective for e.g. depiction of a nude body from is indecent and vulgar for some but for some, it is an artistic expression to Savoured by one Andy all. Where such a dichotomy exists it is important that a holistic view should be undertakes as any narrow interpretation of statue may lead to miscarriage of justice. It would be more if one were dealing with the vexations question of cyber obscenity'. Believing and interpreting the 'cyber obscenity' is an extension of 'physical obscenity' would be fallacious.

**Defining Obscenity**

It is important that in order to have broader perspective it would be worthwhile to trace the historical development of 'test for obscenity' under various jurisdictions:

The test of obscenity was first laid down in Regina v. Hicklin [7] as the tendency "to deprave and corrupt those whose winds are open to such immoral influences and into whose hands a publication of this sort may fall" and it was under stood that this test would apply only to isolated passage of a work. Those "whose minds are open to such immoral influences" primarily meant the young: as Lord CJ Cockburn explained in the Hicklin opinion, the danger of prurient literature persons of more advanced year, thoughts of most impure and libidinous: of character" This view was a precedents for U.S. anti-obscenity legislation beginning with the Comstock law of 1873, which broadened the 1865 Mail Act essentially to its present form by providing fine and imprisonment to any person mailing or reviewing "obscene," "level" or " Lascivious" publications.

The test was slightly modified in United Sates v. One Book [8] entitled "Ulysses" the superior court held that the criterion for obscenity was not the content of isolated obscene passages but rather "whether a publication taken as a whole has a libidinous effect"

The Roth v. United States [9] the U.S supreme court tendered a basic redefinition of obscenity: "whe6ther to the average person applying community standards, the

dominant them of the material taken as a whole appeals to prurient interest:"

With the enactment of the obscene Publication Act, 1959 of UK, the definition of obscenity has been articulated as the tendency to are likely to said, see or hear the contents of the publication rather than those into whose hands the publication may accidentally fall. But even after this enactment the test for obscenity in U.K is still based on the perceived vulnerability of the likely audience for example, capacity of the 'violent' bubble gum cards to "Deprave and Corrupt" the youthful clientele.

**Miller Test**

Where as in Miller v. California [10] the U.S.S.C declared that the states might prohibit the printing or sale of works, which appeal to prurient interest in sex, which portrary sexual conduct in a potently offensive way, and which taken as a whole, do not have serious literary, artistic, political or scientific value". It held that the definition of "Prurient" should be that of "the defence average person, applying contemporary community standard" and that it would be no defence for a work to have some "redeeming social value". The test is there force not the effect of material, but whether it contravens locally determine standards of acceptable sexual depiction.

In Miller v. California the U.S. supreme court set out a there prong test for obscenity, called the 'Millar test':

1. Whether "the average person," applying contemporary community standards would find the work, taken as a whole, appeals to the prurient interest;
2. Whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by state law;
3. Whether the work, taken as a whole, taken serious, literary, artistic, political or scientific value. It important to mention have that the third – prong of the Miller needs a more objective assessment based on a reasonable person test.

As it was held in Pope v. Illinois [11] that the proper inquiry was not whether an ordinary remember of any given community would find serious value in the allegedly obscene material but whether a reasonable person would find such value in it, takes as a whole. Thus, we should reiterate that the factor and standards for obscenity vary greatly depending on the culture of the state, city or town or for that matter foreign country. This make it virtually impossible for a provider and others to determine, with any degree of predictability. Whether the material they distribute, transmit, post and so on would be deemed obscene.

**Test for obscenity in India**

The Ranjit Udeshi [12] case established a modified version of the Hicklin test as the test for obscenity in India. The super me court has observed that the test of obscenity laid down by Cockburn C.J. should not be discarded it held.

"That the test of obscenity to adopt in India is that obscenity without a preponderating social purpose or profit cannot have the constitutional protection of free speech and expression and obscenity in treating sex in a manner appealing to the carnel side of human nature or having that tendency. The obscene matter in a book must be considered by itself and separately to find out whether it is so gross and its obscenity so decided that it is likely to deprave and corrupt those whose minds are open to influences of this sort and into whose hands the book is likely to fall. In this connection the interests of our contemporary society and particularly the influences of the both on it must not be overlooked."

I further interpreted the word "obscene," as that, which is "offensive to modesty or decency, loud, filthly and repulsive". It unhelped the constitutionality of S/292: IPC holding it constitute a reasonable restriction on the right to freedom of expression Under Article 19(2) of the constitution in the interest of decency and morality.

In Samaresh Bose v. Amal Mitra [13] the court held that "the concept of obscenity would differ from country to country depending of the standards of moral contemporary soceity". The court differentiated between "vulgarity" and "obscenity": A vulgar writing is not necessary obscene. Vulgarity arouses a feeling of digust and revulsion and also boredom but does not have the effect of depraving, debasing and corrupting the morals of any reader of the have, where as obscenity has tendency of deprave and corrupt those whose winds are open to such immoral influences.

It is clear from the aforesaid pronouncements that the supreme court has been following the "likely- audience" test a clear departure lies in the wording of S/292(1) of IPC, which speaks of "tend to deprave and corrupt person who are likely, having regard to all relevant circumstances to lead, see or hear the matter contained of embodied in it"

In Director General of Durdarshan v. Anand Patwardhan [14] the Hon'ble Supreme Court once again endorsed Miller test as a basic test for obscenity,

Further in Ajay Goswami v. Union of India [15], the Court observed that the test for Judging a work should be that of an ordinary man of common sense and prudence and not an "out of the ordinary or hypersensitive man" In Judging as to whether a particular work is obscene regard must be had to contemporary mows and national standards. While the Supreme Court in India held. Lady Chatterley's lover to be obscene in England the jury acquitted the publishers finding that the publication did not fall foul of the obscenity test. This was heraled as a turning point in the fight for literary freedom in UK. Perhaps "community mores and standards" played a part in the Indian Supreme Court taking a different view from the English jury. The test has become somewhat outdated in the context of the internet age which has broker down traditional barriers and made publication from across the globe available with the click of mouse.

**Publication of obscene Information in electronic Form**

Publication is defined as "the action of making publicly known". The Supreme Court held in Bennett Coleman & Co. V. Union of India [16] that "Publication means dissemination and the circulation". In the context of internet, the term Publication includes dissemination, storage and transmission of information or data in electronic form.

In general if a book, magazine or an article is obscene, it is an offence to publish it or sell the publication for gain. The question is when 'obscene publication occurre in the internet environment? does Is the information said to be published when data is created or stored in the computer/ Web servers hard disk, retrievable storage medium or when it is transmitted to the end user?

Amend the Law related to obscene Publications

The obscene Publication Act, 1959 of U.K. Provides answers to the Aforesaid question.

The "Publisher Under Section 1 (3) of the obscene Publication Act, 1959 is the one who in relation to obscene material

(a) Distributes, circulates, sells, letson hire, gives or lends it or who offers for sale or for letting on hire or.
(b) In the case of an article containing or embodying matter to be looked at or a record, shows, plays or projects it, to be looked at or a record, shows, plays or projects it, or where the matter is data stored electronically, transmits that data.

The amended definition includes the act of making obscene material available for electronic transfer or downloading to any other person who is able to access and cope that material.

For example in R.v. Fellows Arnold [17] the defendants argued that the act of placing material origin Internet site could not be regarded as a form of distribution or publication the court of appeal however held that while the legislation required some activity on the part of the 'Publisher', this seemed to be amply provided by fact that one of true appellants had taken 'whatever steps were necessary not merely to store the date on his computer via the Internet. He corresponded by e-mail with those who sought to have access to it and he imposed certain condition before they were permitted to do so

In R v. Graham Waddon [18] court of appeal the defendant was charged with publishing obscene articles under obscene Publication Act, 1959 as he had maintained a commercial website featuring explicit image in the United States. He was successfully prosecuted for publishing and obscene article, including its electronic storage and transmission under S. 3(1)(b) of the said Act.

The irony is that even though publishing or distribution of obscene publications may be illegal within the UK under the Obscene Publications Act, 1959, Possession or within the context of the Internet, browsing or spoofing through obscene content is not on illegal activity of unseating adults.

**Apply in the Miller Test**

One of important requirement under the Miller Test has been that the material be viewed in the context of the relevant local "co temporally community standards". The question that arises is, which community's standards are to be used? Will it be the Community standards of the community from where the transmission originated or where it was downloaded? Thus Material deemed obscene in one community might escape the 'black mark' in another. That is applying Miller Test to adjudge online obscenity would be full of possibilities.

In United State v. Thomas [19] "The defendant was operation the Amateur Action Computer Bulletin Board system (AACBBS). He used to convert, by means of a scanner, sexually explicit magazine Picture into computer files and later sell them to the subscribers. Against the complaint of Tennessee court for violating obscenity Laws. The court held that it is well established that: venue for federal obscenity prosecution lies, "in any district form, through or into which" the allegedly obscene material moves. This may result in prosecution of persons in a community to which they have sent materials, which are obscene under that community's standards though the community from which it is sent would tolerate the same material.

Thought the Miller Test has been used successfully to convict perpetrators of obscenity in electronic form, but it is important that the three prongs of the test must not be applied in a selective manner. An over emphasis on 'contemporary community's standards would be highly damaging and may result in the Miscarriage of Justice

**Section 67: Publishing of Information which is obscene in electronic form**

The ingredients of offence under the aforesaid section are:

(a) Publication or transmission in the electronic form.
(b) Material lascivious or appeals to the prurient interest
(c) Tendency to deprave and corrupt persons.
(d) Likely – audience
(e) To said, see or hear the matter contained or embodied in electronic form.

The word 'publication has not been define under the Act, Thus as discussed above, Publication or transmission in the electronic form includes dissemination storage and transmission of information or data in electronic form and in order to comprehend the meaning of electronic form" as defined S. 2(1) (r) properly, due reduce should also be gives to the definition, like "information".

The section advocates that the 'obscene material in electronic form must be considered by itself an Separately to find out whether it is so gross and its obscenity so decided that it is likely to deprave and corrupt those whose minds are open to influences of this sort and into whose hands the Obscene material in electronic form is likely to fall.

The aforesaid section like S. 292(1), IPC does not make knowledge of obscenity an ingredient of the offence, thus to escape criminal charges, all has to prove his lack of knowledge of publication or transmission of obscene information in electronic form. More over though Publication or transmission of obscene information may be illegal but mere possession browsing or surfing through obscene content is not an illegal activity.

Another missing link in the section has been the lack of exceptions as detailed inS.292 IPC i.e. the exception which are available on account of public good, religious purposes etc may not be available if such publication or its transmission is in the electronic form. It should be noted that under no circumstances any offence ululated to obscenity in electronic form should be tried under S 292 IPC as S 81 of the Information Technology Act, 2000 states that will have on overriding effect:

"The provisions of this Act shall have effect not withstanding anything inconsistent therewith contained in any other law for the time being in force."

The punishment provision under S67 of the act is for more stringent that what is being given under S/292. IPC Thus any attempt to mix and match S 67 of the Act and S 292 IPC would create unnecessary confusion may also result in miscarriage of justice.

Offence related to 'obscenity in electronic form should be tried under provision of S/67 only and any attempt to import provision of S/67 only and any attempt to import provision of S292 IPC would tantamount is disregard of the legislature intent behind the Act.

It is important that while interpreting this Section the court may exercise the interest of our contemporary society and particularly the inference of the 'Obscene material in electronic from quit. For this purpose even the state government may have to apprehend perpetrators of 'cyber obscenity' by invoking local state legislation's accordingly.

In Parkash (Dr) v. State of Tamil Nadu [20] Dr. Parkash, the petitioner, was detained under S3 (1) of the Tamil Nadu Prevention of Dangerous Activities. Of bootleggers, Drug offenders, Goondas, Immoral Traffic Offenders and slum Grabbers Act.

The main ground of detention against the petitioner were that the was indulging in offence under 61 of the Information technology Act, 2000. SS. 4 and 6 of the Indecent repres entation of Women (Prohibition) Act 1986 and U/S 27 of the Arms Act, 1959. The petitioner challenged his detention under Art 32 of the constitution of India.

The petition was dismissed, as the Supreme Court did not find much writ in the plea that the delay of two days in furnishing translated copies of documents had caused any perjudice to the defence. It held that the content of the letter received from members of the public pro bono publico were not extraneous of irrelevant

The issue related to publication or transmission of obscene information in electronic form has to be also looked from the perspective of extra-territorial jurisdiction and internet technologies, keeping in view that 'Obscenity' is not longer a local and static phenomenon. It is now global and dynamic in nature are thus need strict interpretation of statue.

**Offence: Beach of Confidentiality and privacy**

The Meaning of the words confidentiality and 'privacy' are somewhat synonymous. Confidentiality involves a sense of expressed or implied contractual obligation. It may also exit independently of any contract, on the basis of an independent equitable principle of confidence. Privacy is the claim of individuals, group or institution to determine for there selves when how and to what extent information about then is communicated to others. Others like Gavison are critical of the ability to control personal information, as being a determinant of the definition of privacy precisely because a dependence on subjective choice wakes both a realization of the scope of the concept and provision of legal protection problematic. Right to privacy is more of all implied obligation. It is the 'right to be let alone'

In the legal parlance, the issue of confidentiality comes up where an obligation of confidence between a ´data collector' and a 'data subject' this may flow from a variety of circumstances or in relation to different types of information which could be employment, medical and financial information. An obligation of confidence gives the data subject the right not to have his information used for other purposes or disclosed without his permission unless there are other overriding reasons in the public interest for this to happen. This is, where an obligation of confidence arise it is unlawful for a data user to use the information for a purpose other for which it was approved

**Law of Privacy: an Indian Perspective**

The constitution of India has not guaranteed the right to privacy as a fundamental right to the citizen but nevertheless the supreme court has come to the rescue of common citizen, time and again by construing "right to privacy" as a part of the right to "protection of life and personal Liberty."

In fundamental right "to freedom of speech and expression" as enumerated in Article 19(1)(a) comes with reasonable restrictions imposed by the state relating to

1. Defamation
2. Contempt of court
3. Decency or morality
4. Security of the State
5. Friendly relation with foreign States
6. Incitement to an offence
7. Maintenance of the sovereignty and integrity of India.

Thus right to privacy is limited against defamation, decency or morality.

The right to privacy could also be read into article 21 which state that 'no person shall be deprived of his life or personal liberty, the supreme Court has observed that "Those who fell called upon to deprive other persons of their personal liberty in the discharge of what they conceive to be their duty must strictly and scrupulously observe the forms and rules of the law" I Ram Narain v. State of Bombay 1952 SCR 652

In Kharak Singh v. State of Uttar Pradesh [21] where the appellant was being harassed by police under Regulation 236(b) of UP Police regulation, which permits for the domicile, visits at right. The Supreme court held that the Regulation 236 is unconstitutional to include, " right to privacy" as a part of the might to "Protection of life and personal liberty" in fact, it was the minority view expressed by injustice, Subba Rao that equated 'Personal liberty' with privacy. He observed that' concept of liberty in Article was comprehensive enough to includes privacy and head a person's house, where he lives with his family is his 'castle and that nothing is more deleterious to a man's physical happiness ad health than a calculated interference with his privacy."

In Gobind v. State of Madhya Pradesh [22] "domiciliary visits and picketing by the police should be reduced to the dearest cases of danger to community. Security and not routine follow up at the end of a conviction or release from prison or at the whim of police officer. In truth, legality apart, these regulations ill accord with the

essence of personal freedoms and the state will do well to revise these old police regulations verging perilously near of unconstitutionality."

In fact Mathew. J. Sated the law in following words. ".... Privacy dimity claims deserve to be examined with care and to be denied only when an important countervailing interest is shown to be superior. If the court does find that a claimed right is entitled to protection as a fundamental privacy right a law infringing it must satisfy the compelling state interest test.....privacy primarily concerns the individual. It their fore relates to and overlaps with the concept of liberty. The most serious advocate of privacy must confess that there are serious problems of defining the essence and scope of the right. Privacy interest in autonomy must also be placed in the context of other rights and values".

Any might to privacy must encompass and protect the personal intimacies of the home, the family, marriage, mother hood, procreation and child. Rearing....."

In State v. Charulata Joshi [23] the Supreme Court held that: the constitutional right to freedom of speech and expression conferred by article 19(1) (a) of the constitution which includes the freedom of the press is not an absolute might. The press must first obtain the willingness f the person sought to be interviewed and not court can pass any order if the person to be interviewed expresses his unwillingness".

In R. Rajagopal v. State of Tamil Nadu [24] where the question was.

(1) Whether a citizen of this country can prevent another person from writing his life story or biography.
(2) Whether freedom of press guaranteed by act 19(1) (a) entitle the pres to publish such unauthorized A/C of a citizen's life and activities. And if so to what extent and in what circumstances?
(3) Whether the public officials, who apprehend that they or their colleagues may be defamed, can impose a prior restraint on the press to press such Publication?

**Justice B.P Jeevan Reddy observed that:**

(1) The right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. It is a "right to be let alone". A citizen has a right to safeguard the privacy of his own, his family, marriage, provocation, motherhood, child bearing and education among other matters. None can publish anything concerning the above matters without his consent. Whether truthful of otherwise and whether laudatory or critical. It he does so, he would be violating the right to privacy of the person concerned and would be liable in an action for damages.....
(2) The rule afore said is subject to the exception, that any publication concerning the aforesaid aspects becomes. Unobjectionable if such publication is based upon public records including court records. This is for the reason that once a matter becomes a matter of public record the right to privacy no longer subsists and it becomes a legitimate subject for comment by press and media among others.....
(3) ..... In the case of public officials, it is obvious, right to Privacy, or for that matter, the of action for damages is simply not available with respect to their acts and conduct relevant to the discharge of their official duties. This is so even where publication is based upon facts and statements, which are not true, unless the official establishes that the defendant (member of the press or media) to prove that he acted after a reasonable verification of the fact it is not necessary for him to prove that what he has written is true....

The court held that the petitioners have a right to publish what they allege to be the life – story /autobiography of Auto Shankar insofar as it appears from the public records even without his consent or authorities. But they go the beyond that punish his life story. They may be induce it right to privacy then they will be liable for the consequence in accordance with law. Similarly, the state or its, officers can not the or restraint the said publication.

In the People's Union for Civil of Liberties v. Union of India [25].

The supreme court held that the telephone tapping, by government under S.5(2) of telegraph act of amount the information the article right to privacy of is a part of the right to life and person liberty the enshrined under the article 21 of the constitution of one of task the given case the constitute a right the privacy. Article the 21 of attracted, the said the right of right curtailed, except the according the procedure, established the right to privacy. By itself has not been identified the constitution. As a concept it may be too brood the moralistic of define it judicially. Whether right to can be claimed or has been infringed the in a given the depend the upon the facts of the said act. But the right to hold the telephone of conversation in the privacy of one's home the office without interference can be certainly by right to privacy, conversation of on the telephone are often of the an intimate and confidence the man life. Telephone the conversation the important fact of mans private the life. Right to privacy. Would be certificate the officer. Telephone tapping in the privacy of one's hone the constitution of topping would thus, infract the attitude the 21 home of officer. Telephone topping would thus, infract the attrite producer India unless it is permitted under the producer establish by law:

Another dimension to right to privacy was added in Mr. X v. hospital Z [26], Blood was to be transferred to another but the he was test HIV at the responds hospital on the also the fissure the fact the applicant proposed the marriage moreover, the was severally accepted, proposed called off, ostracized by the community of criticised one was also the National consumer Disputes of Redresses Commission the damage against the responds the g round that the information of required the under medical ethics. To be kept the secret was disclosed the applied the could seek his remedy the civil court.

Before the supreme court the appetent the contended. The prime of duty of care applicable the person in medical profession included the duty to maintain confidentially and that the said the duty had to a correction right vested in the patient that ever come to the knowledge of the doctor would not be divulged the appellant the added that for the violating the duty as well as the for violating

appellant the damages to the appealer the supreme court while rejecting the apple ant continuous hold that the right to privacy the has been called the out of the provisions article 21 and other right road with director principles of state policy, right of privacy may be with directive of from contract also arise out of the participate the matrimonial, and or event political, doctor the relationship the though basically comers is professionally, the morally and facts may amount to the invasion of the right of one person right to be sometimes alone, right however the is not obsolete and may be low fully restricted for the prevention of crime, disorder or protection of health or morals of protection the right and freedoms of there,.

There is a clash of fundamental right or is this case right the privacy of one party as art of right to life and right to tea a healthy life a another the article the right which they would alone a enforced through the, process public interest would alone a be enforced the through the consideration can't of court, for the reason the moral the consideration by the courtroom, they have to be hall known the courtroom, they have to sensitive, In the sense that they must keep their finger firmly of in pulse of the accepted the fingers day.

IN Shardha v Dharampal [27] it was the by supreme court that the right to privacy in the art 21 of constitution of not an absolute right. There was the a conflict of b between the right to the parties, that right which advance public morality would prevail

In District Registrar and Collector v. Canara bank [28]

It was held by the supreme court that the exclusion the illegitimate intrusions into privacy depends on the nature of right being asserted and the way n the which it is the brought into the asserted and the way n which the context of becomes crushed the play in it is the point that the context becomes the relevant the defiling the searches and seizures the instance of the state.

**Privacy in the technology Driven word**

Privacy in the technology deriven the world is a difficult of proposition of technology has become a kind of the double the edged sword, the had it equips the person to the safeguard the privacy and to on the other of helps in the blowing the privacy cover one may have had,

There are the means to capture the digital footprints. Of the user of who is browsing the internet the various of personal the reasons. Who is the browsing the all begins with the capturing the when by the communication link is the made over the identified as it been given a unique and address. By ISP. It is represented by the browse visit to site of sends a email the 255. Whenever the person browse, visit to site of IP address behind. It is possible either by the searching IP registration databases of by conducting or trace route to determine an approximate physical of an address. Other surveillance technology being widely used are

(a) Cookies
(b) globally unique and identifier guild
(c) web bugs
(d) email or document bugs
(e) spyware
(f) online digital profiting

a. Cookies:- A cookies is a block of text which the website place in the file on a computer the hard disk of a person the track his website the label him as a particular user has registered the him by name or address unless he has information or set up the preference in his of browser. To do so automatically some of these website are affiliated strum of customized the advertisement of includes junky mail too.

Cookies, are sometimes of referred to as necessary of envies they the support and facilities of commerce the activities, website the key to the personalization of the web. Some the take the context of the user the before the placing to cookies of the user hard disk.

b. **GUID: -** Globally unique Identifier is a software hat of is enabled the computer Hardwar. It was the be head reputedly of across the network. For example of one may be find GUID of Ethernet the cards, used to local the Area network. The result would be eaves dropped of all the computer connected through Lan.
c. Web bugs:- web bugs are being increasingly used by the online advertisers to create a users data base. A web of page that a part of a banner ad a website the page that a person is viewing. The instance would course the person's browser. To transit the advertisers server the URG of the page the server is able to the web page the person is about the view banner ad that it thinks will interest of the person. Surprisingly that it one ways exchange surprisingly. This is a one way exchange of information and it occurs even the though the person has not clicked on the banner ad.
d. Email and document bugs:- It is the good too in the hands of a sender of an email and document to know whether the recipient has read the email the or spend the document the electronic the document the opened the document web bugs they call home would be laden with the date the message the was opened.
e. Online digital profiling:- International online advertising companies insert add on web pages with the cookies of tagged on them. Once clicked they start building up the users how advertising companies, known the profiles build and use it to the put add targeting him on the partner, sites. Also that has been an increasing use of profiting software the that reads. The uses online activity and recommends other similar products.
f. Spy ware:- some software the develops have included the ode backdoor the adware the drive the user's computer transit information back to the software the developer the via internet. Content the one user that is tailored to the information the scan the user the adducing the information the profile the developers have been be used for market in purpose. Several develops of the discovered the using have been new strains the becoming increasing the insidious and there are the new can do the from. Generally annoying pop up advertisement to collecting of password and credit cord number.

Protecting privacy in the technology world driver is the mirage. Hence is would be important to examine how the

question of Technology act, 2000 has dealt with the question of the privacy digital medium.

**Section 72 penalty for breach of confidentiality and privacy**

The aforesaid section has a limited application of only. It confides power the under this act, rules or the regulation made

a. The controller of certifying authorities
b. The deputy certifiably assistant controller or certifying power authorities
c. Licences certifying authorities of and auditors of
d. The adjudicating officer {s.46}
e. The presiding officer of the cyber Appellate Tribunal (Ss 48-49)
f. The registrar of cyber appellate tribunal (R.26)
g. The register the cyber tribunal {s. 56}
h. Network service provider {s. 79}
i. Officer deputy supretendent of police

To secure the access of any electronic record, book, registrar, of correspondence of document of other materiel the. The idea of the behind aforesaid section in that the person the who has secured accords of second any such if shall not take unfair the advent age in the disclosing the third plan without Any consent the disclosing the party an obligation of the confidence arises at the date collector the date subject the case of unauthorised the such information said person the punished the with year with the which may be extend the on lakh rupees of with both.

As highlighted in the aforesaid discussion the issue of the confidentiality of the privacy as in of the act should be read along with the right to freedom the restriction of imposed of act 19 of data subject the take advantage the article the click the person of person shall be depraved his life or personal liberty except according the procured the established the law.

**Offence related to digital signature of certificate**

A digital the signature of certificate is important of trust identifying the subscriber the of network, this instruments of trust the bound the play on the important the role in commerce of both of macro of business got 2 of business the micro the instrument of truss remains the protected the law.

**Penalty of the publishing the signature of certificate the certain the section 73.**

Publication is defined as the action foot he making publish of know, the supreme the court held the Bennett Coalmen and co.

a. A Publish or transmission of a digital signature of certificate
b. B Prior knowledge the of fact that

1. That certificate the authority of the listed in the certificate has not issued it.
2. he subscriber listed in the certificate the not accepted it.
3. The certificate has been network or suspended

Under the scheme of the both the certificate the authority of and the subscribe have to accomplish to task of the publication or transmission of digital signature certificate under S/36(b) of the Act a certifying authority while issuing a Digital Signature certificate is to certify that it has published the digital certificate is to or otherwise the made it available the such person relying the otherwise the made it subscribe the accepted it.

Similarly the under 5.41 of the act of subscriber the shall be deemed to have accepted the digital the signature certificate the publisher the authorised the publication of a digital signature of certificate.

a. To one or more person
b. In a repository or otherwise the demonstrates of his approval of the digital signature of certificate the any manner.

It is been provided under the rule 23 that the certifying authority shall provide a reasonable opportunity for the subscriber to verify the content of the digital signature certificate the before it is accepted the by him. Is further that upon the of acceptance of the used. Digital of signature by the subscriber the certificate the shall publish a signed copy of the digital signature the certificate the in a rule 23 of.

Also under the sub section knowing the publication of the a digital of signature the of certificate a authority of the making it of the available to any other the person, is an offence, also any the revoked or suspended is on offence. Also any the revoked the part of the certificate revocation as the case notice of the such suspension or revocation as the case of the in the repository specified the digital may be, the certificate for publication of the such notice, may make the certifying of authority such notice.

S.39 may make of certifying authority liable the sub section of further the states not be publication to a digital signature of the certificate is for the purpose the verifying the digital of signature shall be made the out, the sub section he further the states that the penalty of for punishing the aforesaid the and the bible offence, The aforesaid section is to within punishment or with fine which may extend to two years with fine, which may extend the tax lakh rupees with both,

**Section 74: publication on for fraudulent purpose**

A digital signature of certificate in an important the identifying the subscriber over the network. The DSC trust of binding the linkage bet the subscribe and the issuer. As discussed in the previous the chapter a digital signature certificate the is product of PKT system, of which only confine the information of like the subscribe the but also certifies other relevant information like the subscriber public key and bona fides of the issues of the certificate. This about the identity of the subscriber is digital of relying the party, who put implicit trust and accuracy the said certificate.

In the aforesaid the section has once thus is both the certifying the authority and subscribe not a create. Publish the otherwise the make available the signature for any fraudulent and purpose.

One point out should not be missed is that any fraudulent and unlawful would be taking place on any of the computer of resource [S.2 (1) (k)] of the fraudulent the unlawful process the certain information contained the digital signature certificate the further the criminal offence.

In the context of digital medium, the term publication of includes of dissemination of the storage the transmission information data in electronic the form. Publications of the fraudulent the purpose the and transmission of modified the digital signature of certificate the with the intent to commit fraud, penalty of purpose of digital of signature of certificate the of purpose has been made a non-cognizable the with imprisonment of aforesaid the of offence of punishable the years or the which we extend the one lakh rupees of with both.

By virtue the section 73 &74 of the digital of signature of the certificate the accorded the status of electronic the record the sense of purpose the will be considered the criminal of offence. A digital of signature certificate is a digital of subscribe of as in instrument of the must, of identifying the he subscribe the over the network.

**Offence contravention of Committed of outside of India.**

The act of understand the reach of the criminals, who with the attack of the mouse of the key stock fat eared in the position, of the computer, of system the network of the located anywhere the world These thread the very real ad universal in origin the hence the realization the part of the lawmakers of enact such provisos of so as to enforce jurisdiction that goes beyond the section of limits.

**Section 75 at of the apply for offence of contravention of committed outside India**

The aforesaid take a broader view of cyber crime's of committed by cyber criminals, It is out cohered with the territoriality of the atonality of cyber criminals.

a. Any person irrespective of nationality
b. The said offence or contravention must have been committed against of a computer, computer system or computer network located in India.

In a broad sweep, the act has the adopted the principles of the universal the jurisdictions of the cover both the cyber of contraventions of and cyber the jurisdictions of the specified the offence the result universal of condemnation of those a activities', of requires operation of agreements, of conventions. Though the India is not one of signature of the cyber crime convention, cover both the and cyber offence under the act; _

The jurisdiction of Indian courts on cyber criminals belonging to different nationalities. Moreover the sextradition Treaties, which India has Signed so far, do not cover 'cyber crime' on an extraditable offence. Had India being a Signatory to the cyber crime convention, then criminal, then by the virtue of Article 24 of the said convention the criminal offences as mentioned in Article 2-11 shall be deemed to be included as extraditable offences in any extradition treaty existing. Between or among the parties. Further the Parties undertake to including such offences as extraditable offences in any extradition treaty to be concluded between or among there.

To believe that the convention would be a panacea to the problem of extraterritoriality as erroneous. Cyber crime involving computer, computer system on computer network, geographically spread across many countries may give rise to difficult jurisdictional issues. A lot will depend on the nature of crime, the 'point' of origin as. Well as 'point of disruption' and the extent of economic loss.

In R v governor of Brixton Prison and another ex parte levin 35 where citibank faced the wrath of a illegal transfer of funds from customers account into accounts of the hacker, eater identified as Vladimer Levin and his accomplices. Levin was arrested on tshe united kingdom and subsequently extradited to the united states.

One of the most crucial jurisdictional issue was the 'Place of origin' of the cyber crime. The defence argument was that the criminal act occurred in St. Petersburg at the moment when levin pressed particular keys on the keyboard resulting into fraudulent citibank transfers, hence levin to be tried as per the Russian law. The complainant argued that the place where changes to the data occurred, constituted the place where the offence took place.

The court held that the real- time nature of the communication link between levin and citibank meant that levin's keystrokes were actually occurring on the citi bank computer.

It is thus important that in order to resolve disputes related to jurisdiction, the issue of terrioriality and nationality must be replaced by a much brother criteria embracing principles of reasonableness and fairness to accommodate overlapping on conflicting. Interests of states, in the spirit of universal jurisdiction.

**The Issues in online Defamation**

**Defamation**

Black's law dictionary

Defamation is defined as "an intentional false communication either publish or publicly spoken that injures another's reputation or good name" Defamation includes the common law torts of libel ( involving written or printed statements) and slander (involving oral statements). Significantly both and libel as slander could be committed via internet medium.

Defamation is an intrinsically personal wrong. The gist of defamation is actual or presumes damage to reputation flowing from publication (or communication) of in traditional libel cases "publication" is generally referred to as "the date on which the libelous work was placed on sale or become generally available to public". It has following ingredients;

(a) Publication of a statement;
(b) Statement makes reference to the plaintiff.
(c) Statement is communicated to some person or persons other than the plaintiff himself;
(d) Statement reaches the plaintiff;
(e) Statement causes actual or presumed damage to the plaintiff;

The question is does one encounter similar 'ingredient' when defamation occurs in internet medium here, the only difference is that the tort of defamation occurs when the defamatory imputation is published in electronic form, everything else remains the same.

**It All Begins with Publication**

Publication is defined as the action of waking publicity known" In the context of internet the term publication

includes dissemination, transmission and storage of inf. or data on electronic from.

In order to construe a relationship between defamation and publication in the internet medium, one may have to answer following questions;

(A) When a publication takes place
(B) How a publication takes place
(C) Where the publication takes place
(D) Who would be held responsible for the publication of the allegedly defamatory statements.

A. When?

Publication occurs when the contents of the publication, oral, spoken or written one seen and heard and comprehended by the reader or hearer. From the point of view of plaintiff, the process of publication is complete, when the communication reaches him.

In Godfrey v Demon Internet Ltd. 4AIIER342 high court 4AIIER 342 HC

The defendant ISP carried the newsgroup 'soc. Culture Thai' and stored posting within that hierarchy for about a for night during which time the posting was available to be read by its customers. On 13 January, 1997 some on unknown made a posting in the US in the newsgroup. This posting was squalid, obscene and defamatory of the plaintiff who was resident in England. On 17 January 1997 the plaintiff sent a letter by fox to the defendants, requesting them to remove the posting from their used news server. The defendants could have obliterated the posting after receiving the plaintiff's request, but it remained available until its expiry on or about 27 January 1997. The plaintiff claimed damages for libel in respect of the position after 17 January 1997. The time when he affirmed to the ISP that the communication had indeed reached him.

Morland, J. Ruled:

"In my judgement, the defendant, whenever it transmits and whenever there is transmitted from the strong of its news a defamatory posting, publish that position to any subscriber to its ISP who is accesses the newsgroup containing that posting. Thus every time one of the defendant's customers accesses 'Soc culture Thai' and sees that posting defamatory of the plaintiff ;there is a publication to that customer."

B. How?

How is the publication has occurred i.e. in what from publication has happened ? It is an important issue on the techno-legal driven environment It looks into the mode of publication (or transmission) whether audio, video, textual or multimedia, Internet publishing is in electronic form. Instances of defamation in 'electronic from' include generating, sending or receiving 'defamatory' email, online bulletin board Massage, chat room message, music, downloads, audio files, screaming videos digital photo graphics etc. On the internet.

C. Where?

where the publication has occurred is not easy to define as a defamatory statement can be "published" anywhere in the world where there is access to the Internet, here the issue is whether due process of law would be served by hauling a defendant into a particular jurisdiction simply because he has posted information that can be accessed anywhere in the world.

In the context of Internet, it is not necessary for the plaintiff in all cases to prove directly that the defamatory statement was brought to the actual knowledge of anyone (some person or persons other than the plaintiff himself) publication is only established if the plaintiff makes it a matter of reasonable inference that the publication was accessible in every jurisdiction where it can theoretically be accessed. So as a matter of reasonable inference, it can't be assumed that any site put on fact accessed everywhere then can publication be assumed to have taken place.

In R v. Graham Waddon The defendant was charged with numerous counts of publishing obscene article contrary to 5.2 (1) of UK's Obscene Publication Act, 1959, the defendant had created pornographic images, which were illegal under the UK's Obscene Publication Act. He ran a series of sites based in the us, hosting them on a US based internet service provider there images were accessible to anyone in the world via the Internet who become a subscriber by giving credit cards details. He was charging UK customers 25 pounds a month for access. The subscriber was given a password and could long into the various websites to obtain the images. IT was submitted on behalf of the defendant that, because the Internet publication had necessarily occurred abroad, therefore. The instant court did not have jurisdiction.

Hardy Christopher, J. Held:

"Publishing an Article under S. 1(3)(b) of the 1959 Act included data stored electronically and trans witted person to another Su the lust and case, au act of publication took place when data was transmitted by defendant or his agent to the service provider, and the publication or transmission was in effect still taking place what the data was received. Both the sending court and it was irrelevant that the transmission may have left the jurisdiction in between the sending and receiving."

In Dow Jones and company Inc v. Gutnick on the other hand, the high court of Australia approved the trail court's assertion of an allegedly defamatory article. The article appeared in Barron's which was available to subscribers of wsj.com. Joseph Gutnick, a resident of the Australian state of Victoria, brought a defamation action against Dow Jones in a Victoria, court, Dow Jones argued that the court should decline jurisdiction under the doctrine of forum non conveniens, which would be applicable if the Victoria court was a "clearly inappropriate forum" Dow Jones argued that Barron's online was published in New Jersey, the location of the server host the substantive law to be applied in deciding the case is new jersey law, which would make the Victorian court a clearly inappropriate forum, thus the decision hinged on where the article was deemed ;to be published.

The court held, contrary to Dow Jones's contention that publication of a defamatory statement is bilateral act' in which the publisher makes it available and a third party has it available for his or her comprehension", therefore, the article was published, with respect to Gutnick's cause of action not when Dow Jones placed it on its web server, but only when subscribers in Victoria accessed it she site recorded about 550,000 hits, less than 0.01 per cent of them from people with Australian credit cards. It was not ascertain, able hoe many of these users were Victorian but it was defamation occurred in Victoria, and that Victorian law governed: " It is where that person downloads the material that the damage to reputation may be done Ordinarily then, that will be the place where the tort of defamation is committed " Since jurisdiction in Victoria was proper and Victorian law would be applied, the Victorian court was not a clearly inappropriate forum" and there was no basis for declining jurisdiction.

A person is defamed at the place where publication is made, and in the context of Internet it is the downloading of the information that is a relevant fact for identifying the jurisdiction. The criticism that the plaintiffs may resort to "Forum shopping" in order to bring their claim in a jurisdiction which provides them with a greater chance of success is untenable. Before deciding any case, the court will have to observe whether there exist a substantial with the place where proceedings are instituted.

D. Who?

Who would be need responsible for the publication of the allegedly defamatory statements the ISP or the website promoter? An internet service provider represents an interactive network service, It may provider access to the Internet only or offer a range of additional services. Depending upon its functional attributes, an internet service provider may act as an information distributor (carrier) or 'information publisher".

An information distributor merely acts as a carrier of information (third party content) transmitting 'electronic message' from one place to another, without examining its content the function of an transmit the information but also take reasonable care in relation to the said publication.

It is thus important to, look into the cases, where the court has identified ISP as either information distribution or information publisher.'

In contrast in Stratton Oakmont, Inc. V. Prodigy servs. Co. plaintiffs, of security of investment of banking firm of sued proudly of the company an interactive computer the service the defamatory of the comments boards against party of defamation comments prod bulletin the against the firm's. The court of the held prodigally the strict liability the standards normally the applied the held piggy of the punish of the statement of rejected prodigy claims. Standards usually the reserved thedistribute of the knowledge the than prodigy acted the more like an original the court publisher than a distributors the both became the advertised the practice of screened the edited message the posted its bulletin board the defamation, Indian perception.

**Online Defamation: An Indian Perspective**

In India issue of the defamation has so far the been dealt the under the provision of the Indian penal code 1860 of the code makes no distinction b/w as slander and libel. In define Defamation.

It is has been argued that from the point of the view of application it would be extremely of difficult of enforce section 499:-

Whoever the words, either spoken a or intended the or be read, or by signs or by visible representation of makes or publishes any imputation concerning the any person of intending the harm, of knowing the having reason the to believe that the such imputation of the harm the reputation of the such person is said except in the case hereinafter excepted, the define that person.

The three ingredients are:-

1. Making for the publishing of imputation of concern any person
2. Such imputation of must have been made by
   a. Words, either spoken are intended to be read
   b. Signs
   c. Visible representation
3. Such imputations of must have been made with its intention of having the with knowledge or reason of believe that the harm the repletion of person the conquering the whom made.

The code also the highlights of that defamatory statement of need be punishment. The supreme court of Bennett the Coleman & co. V. Union of India that the publication of means the dissemination and circulation that is communicating defamatory statements o only of the person defamed is not publication.

It is important to note that an essential of differences between the Indian and the English law. Is that the farmer recognize the word spoken, as a made of defamation of the court of Balraj Khanna v. Moti Ram

It is the will be highly of describe of doubt it the actual of word state of now have been used by the accused and which the all to be defamatory of the reported the compliment. The actual of words used to or the statement of made by the reported the vibrations by the statement of words of are few and the statement of is very brier But the few and the word spoken are too of many of the statement of made are too long, of will be the high technology the assist to actual words of and the strive the statement of variation.

The code by the highlight of the defamations could also happen by means of signs or visible representation has included every possible form of defamation including defamation in electronic form as well. Instances of defamation in electronic form including chat room message by the sending or receiving, screenings the of videos, online bulletin board, online chat digital photographic on the internet. Even sending the defamatory SMS, MMS, photograph, videos on mobile phones of would be considered instance of defamation of the electronic the form It is words, the code of official of tackle of online of matter.

**Issue of the jurisdiction**

A claimed the reputation of the will award of damage of only of the play of made. This has always be place where the publication of the made. This is the common was the contract if India the some principle has been adopted publication of takes place written of where the contents of the publications the arid spoken the redder written are seen and the heard, and comprehended the reader or hearer.

In P. Lanksh v. H. Shivappa [29] where are a newspaper the containing of articled of punished at one place and in circuited the sad at other of or an behalf of the accused the responsible of for printing of publishing of newspaper them would be of defamatory of article of all the such places of the defamatory of imputation of made public at several places, then the offence is committed at each of such place.

Exceeding the aforesaid principle of in the environment a publication of would take place where the rest riving the downloaded which the means restricting of live remote computer, of computer system the or computer rework of is it software of driven the process that requires the distributes the or publisher the submitting to the web browser a download request in the form of the uniform resource locater URL once a website is download one any of again the select any of website of download the one many of downloads. The publication of occurs when the thus any of user access of the publication of the user.

It is obligatory that the before delaying whether an online publisher or distributor is liable for defamation under the aforesaid provision by IPC. One should be also take cognizance of the information of technology act 2000. The said section express the legislations of inter of granting of immunity to the network service provider. The immunity is absolute if and only if he proves for any only third party of information that-

1. He had no knowledge the inf. content it is transmitting is unlawful;
2. He had the exercised all the diligence of the prevent transmissions for publication of unlawful of information content.

A network service provider may act a on online publisher of distributor of though the no such categories of have been of identified in the Information Technology Act 2000 In that way the Indian Position is closer to the English law.[S.1(1)(b) and S.1(1)(c) of the Defamation of Act 1996] than the US. Communication of December act, 1996 which forbids the imposition of publisher liability on service provider for the exercise of its editorial and self-regulatory functions.

Information technology act, 2000 play a good role to deal with the offence relating to cyber crimes. It provides the various provisions which deals with the offence which is related to the cyber space. This of chapter deals of offence which is related to the cyberspace and Information Technology Act 2000 and provide the preventive measure to control of this type of offence in India.

**References**


1. System Development Life cycle.
2. Report of United National Commission, 1979.
3. S/1 Computer Misuse Act, 1990.
4. 1986 (83) Cr. APP 54.
5. 1991 (93) Cr. APP 25.
6. 1970 (2) SCC 780.
7. 1868 (3) QB 360.
8. 1934 (72) QB 1957.
9. 1957 (354) US 476.
10. 1973 (413) US 15.
11. 1987 (481) US 497.
12. 1965 (1) SCR 65 SC.
13. 1985 SCC289.
14. 2006 (8) SCC 433.
15. 2007 (1) SCC 170.
16. 1972 (2) SCC 788.
17. 1997 (2) AIIER 548.
18. AIR 2000.
19. 1996 74F 3d 701 (6th cir) Cert.
20. 2002 (7) SCC 759.
21. 1952 SCR 625.
22. 1963SC1295.
23. 1975 (2) SCC 148.
24. AIR 1995 SC 264.
25. 1997 (1) SCC 301.
26. 1998 (8) SC 296.
27. 2033 (4) SCC 493.
28. 2005 SC 186.
29. 1994 Cr.LJ 3510 Kant.