Privacy and surveillance : The Law relating to Cyber Crimes in India

Jitender K Malik*, Dr. Sanjaya Choudhury

*Department of Law, Bhagwant University, Ajmer (Raj.) –India

Jitender_malik@hotmail.com

Abstract:

The concept of crime is not a modern one; it has been in existence since time immemorial. However, the concept and nature of crimes constantly change. The definition of crimes has been changed accordingly. In the 20th century and with the advent of computer, the criminals have changed the mode of committing the crimes from conventional methods to computer based methods. The first recorded cyber crime took place in the year 1820. That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been in vogue since around 3500 B.C. in India, Japan and China. Indian legal system is now in a developed stage; and is enacting the law along with the changing situation. In the age of information technology, a comprehensive cyber law is the need of the hour. The definition of cyber crime is not possible because there are different forms of misuse of information technology. Any particular definition of cyber crime may adversely affect the interest of the large society. Therefore, it is not possible to define the term cyber crime. The conventional definition and types of crime covers almost all cyber crimes; since the basic thing is the same. However, work on the treaty proceeded. This led to the International Convention on Cybercrime in Budapest in 2001; which was signed by thirty countries, including Japan, South Africa, Canada and the US. The convention authorizes a global cyber police force to investigate cyber crime. This meant that investigators had the power to track down network communications and to store intercepted data across countries. For this to work, nations must cooperate with each other by sharing gathered information and evidence related to cyber crime. Additional protocols covering terrorist activities and racist and xenophobic cyber crimes were proposed in 2002. The Convention did not necessarily guarantee that the issue of cyber crime would have an immediate solution. The provisions could come into full effect only if they were approved by that country's national legislature. Despite all of the controversy surrounding the Convention and the surveillance powers given to the nations who adopt it, the treaty is still a step ahead in the capturing and prosecution of cyber criminals. Since then, a plethora of laws have been adopted across the different countries of the world reinforcing them against the threat of cyber crime. Illegal or unauthorized use of a computer system, theft of private data and digital fraud are considered acts of felony in the US. Organizations without a viable network security program can be held responsible for negligence in the event of a cyber attack.

1.Introduction

Cyber crime is a worldwide problem. Various authorities at the national and international levels have attempted a comprehensive definition of the term “cyber crime.” Following are certain important definitions. The Oxford Reference Online defines 'cyber crime' as “crime committed over the Internet.” The Encyclopedia Britannica defines 'cyber crime' as “any crime that is committed by means of special knowledge or expert use of computer technology.” Cyber crime could reasonably include a wide variety of criminal offences and activities. The words ‘cyber crime’ and ‘computer crime’ are used inter changeably in common parlance. The word computer crime has a wider ambit as it entails not only crimes committed on the internet but also offences committed in relation to or with the help of computers. Don B Parker distinguishes between the concepts of ‘computer crime’ and ‘cyber crime’ thus: the former is a crime in which the perpetrator uses special knowledge about computer technology; but the latter is a crime in which the perpetrator uses special knowledge of cyber space. However, this definition is not exhaustive as there are many acts, which can be called abusive activities concerning the computer but they are often not clearly illegal. Moreover, most of the cyber crimes are committed *via* internet; and the definition has no reference to it. Cyber crimes can be plainly defined as “crimes directed at a computer or computer system.” But the complex nature of cyber crimes cannot be sufficiently expressed in such simple and limited term.[1]

The Organization for Economic Co-operation and Development (OECD) recommended the working definition of cyber crime: “computer related crime is considered as any illegal, unethical or unauthorized behavior relating to the automatic processing and the transmission of data.” This definition also cannot cover the border aspects of the real nature of the cyber crime. While defining cyber crime, it only covers the illegal activities pertaining to the data transmission. However, cyber crime not only deals with the data transmission, it includes every illegal activity *via* computer.

The Council of Europe Convention, 2001 includes four different categories of offences under the definition of cybercrime:[2] (i) offences against the confidentiality, integrity and availability of computer data and systems; (ii) computer- related offences; (iii) content related offence; and (iv) offences related to infringements of copyright and related rights. This is not a definition; but an explanation of the cyber crime.

From the above definitions, a conclusion can be drawn that cyber crime is much border and wide term. There are various cyber laws enacted by the various Nations, but no nation can provide a comprehensive cyber law that covers the complete concept of cyber crime. Whenever a person misuses the cyber space to commit any illegal act, it can be termed a cyber crime. India has enacted the Information Technology Act in 2000. But it has not provided any definition of cyber crime.

Cyber Offences under the Indian Penal Code, 1860

In India, the major substantive criminal law is the Indian Penal Code- a complete code which deals with all the offences, including cyber crimes. Therefore, this conventional criminal law is sufficient to deal with all kinds of crimes including cyber crimes. India enacted the Information Technology Act, 2000 basically to regulate e-commerce. The Information Technology Act, 2000 contains wide range of offences such as tampering with computer sources, violation of privacy; publishing obscene material etc. Many of them are already recognized as offences under the Indian Penal Code. Some of them are tabulated hereunder:

	ACTS	OFFENCES UNDER IPC	PROVISIONS OF IPC
1	Sending threatening messages	Criminal intimidation	Section 503
2	Sending defamatory messages	Defamation	Section 499
3	Bogus websites, cyber frauds	Cheating	Section 420
4	Spoofing/Forged e- records	Forgery	Section 463
5	Web-jacking	Extortion	Section 383
6	Pornography	Obscenity	Section 292
7	On-line harassment	Stalking	Section 354-D

The Information Technology Act, 2000

The Act was enacted to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce," which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

In 1997, the General Assembly of the United Nations by a resolution[3] has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL model law, 1996). The resolution recommends *inter alia* that all States give favorable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information. Indian Parliament considered it necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records. Consequently, in 2000, the Information Technology Act was enacted.

2.Objectives of the Information Technology Act, 2000

IT Act, 2000 focuses mainly on three aspects:

(i) Providing legal recognition to the transactions which are carried out through electronic means or use of Internet.
(ii) Empowering the government departments to accept filing, creating and retention of official documents in the digital format; and
(iii) To amend outdated laws and provide ways to deal with cybercrimes.

The following are the objectives of IT Act 2000

(i) To give legal recognition to any transaction which is done by electronic way or use of internet
(ii) To give legal recognition to digital signature for accepting any agreement *via* computer.
(iii) To provide facility of filling documents online relating to school admission or registration in employment exchange
(iv) To enable any company to store their data in electronic storage.
(v) To stop computer crime and protect privacy of internet users.
(vi) To give more power to IPC, RBI Act and Indian Evidence Act for restricting electronic crime.
(vii) To give legal recognition for keeping books of accounts by bankers and other companies in electronic form.

The Information Technology Act, 2000 is a facilitating Act as it facilitates both e-commerce and e-governance. Interestingly, the UNCITRAL Model Law of E-commerce on which this Act is based has made no reference to e-governance. But it was the collective wisdom of the legislature, which saw the necessity of introducing concepts like e-governance in this Act. In fact, the entire Chapter III of the Act is devoted to e-governance and e-governance practices. There are 7 sections in the aforesaid Chapter III of the Act, from section 4 to section 10, which deal with e-governance issues. These sections form the basic law related to electronic governance rights, which have been conferred to the persons and the Government(s) both Central and State Governments. It is applicable to the whole of India, including the State of Jammu and Kashmir. It is important to understand that the Information Technology Act, 2000 is the first enactment of its kind in India, which grants e-governance rights to the citizens of India.

The Information Technology Act, 2000 is an enabling Act as it enables a legal regime of electronic records and digital signatures. That is, in order to be called legally binding all electronic records, communications or transactions must meet the fundamental requirements, one authenticity of the sender to enable the recipient (or

relying party) to determine who really sent the message, two messages integrity, the recipient must be able to determine whether or not the message received has been modified en route or is incomplete and third, non-repudiation, the ability to ensure that the sender cannot falsely deny sending the message, nor falsely deny the contents of the message. The Act provides for Digital signatures, which may be considered functional equivalent to physical world signatures capable of meeting all the fundamental requirements, like authenticity of the sender, message integrity and non-repudiation. Digital signature is a misnomer. It does not mean scanning the handwritten signatures electronically. In fact by applying digital signatures one may actually transform an electronic message into an alphanumeric code. It requires a key pair (private key for encryption and public key for decryption) and a hash function (algorithm).

The Information Technology Act, 2000 is a regulating Act as it regulates cyber crimes. As stated above, cyber crime is a collective term encompassing both cyber contraventions and cyber offences. The Act not only demarcates contraventions from offences, but also provides a separate redressal mechanism for both.

Structure of the Act

The Act totally has 13 chapters and 90 sections (the last four sections namely sections 91 to 94 in the Information Technology Act, 2000 dealt with the amendments to the four Acts namely the Indian Penal Code 1860, The Indian Evidence Act 1872, The Bankers' Books Evidence Act 1891 and the Reserve Bank of India Act 1934). The Act begins with preliminary and definitions and from there on the chapters that follow deal with authentication of electronic records, digital signatures, electronic signatures etc. Elaborate procedures for certifying authorities[5] have been spelt out. The civil offence of data theft and the process of adjudication and appellate procedures have been described. Then the Act goes on to define and describe some of the well-known cyber crimes and lays down the punishments therefore. Then the concept of due diligence, role of intermediaries and some miscellaneous provisions have been described. Rules and procedures mentioned in the Act have also been laid down in a phased manner, with the latest one on the definition of private and sensitive personal data and the role of intermediaries, due diligence etc., being defined as recently as April 2011.

Applicability

The Act extends to the whole of India and except as otherwise provided, it applies to also any offence or contravention there under committed outside India by any person. There are some transactions where the Act is not applicable as detailed in the First Schedule, stated below:

(i) Negotiable instrument (other than a cheque) as defined in Section 13 of the Negotiable Instruments Act, 1881;
(ii) A power-of-attorney as defined in Section 1A of the Powers-of-Attorney Act, 1882;
(iii) A trust as defined in Section 3 of the Indian Trusts Act, 1882
(iv) A will as defined in clause (h) of Section 2 of the Indian Succession Act, 1925 including any other testamentary disposition
(v) Any contract for the sale or conveyance of immovable property or any interest in such property;
(vi) Any such class of documents or transactions as may be notified by the Central Government.

Highlights of the Act

Chapter-II of the Act specifically stipulates that any subscriber may authenticate an electronic record by affixing his digital signature. It further states that any person can verify an electronic record by the use of a public key of the subscriber. Chapter III of the Act details about the electronic governance and provides inter alia amongst others that where any law provides that information or any other matter shall be in writing or in typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is (a) rendered or made available in an electronic form; and (b) accessible so as to be usable for a subsequent reference The said chapter also details the legal recognition of digital signatures.

Chapter IV of the Act gives a scheme for the regulation of certifying authorities. The Act envisages a Controller who shall supervise the Certifying Authorities as also laying down standards and conditions governing the Certifying Authorities. The Controller will also specify the various forms and content of digital signature certificates. The Act accepts the need for recognizing foreign certifying authorities and it further details the various provisions for the issuance of license to issue digital signature certificates. Chapter VII of the Act details the scheme of things relating to digital signature certificates. The duties of subscribers are also enshrined in the Act.

Chapter IX talks about penalties and adjudication for various offences. The penalties for damage to a computer system have been fixed as damages by way of compensation not exceeding rupees one crore. The Act talks of appointment of an officer not below the rank of a Director to the Government of India or an equivalent officer of a state government as an Adjudicating Officer to judge whether any person has made a contravention of any of the provisions of the Act. The officer has been given the powers of a civil court.

The Act in Chapter X talks of the establishment of Cyber Regulations Appellate Tribunal, an appellate body where appeals against the orders passed by the Adjudicating Officers shall be preferred. Chapter XI of the Act talks about various offences. These offences include tampering with computer source documents, publishing of information that is obscene in electronic form and hacking. The Act also provides for the constitution of the Cyber Regulations Advisory Committee which shall advice the government as regards any rules or for any other purpose connected with the said act. The Act also has four Schedules which amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934 to make them in tune with the provisions of the Information Technology Act, 2000.

3.Salient Features of the Information Technology Act, 2000

- Extends to the whole of India
- Authentication of electronic records
- Legal Framework for affixing digital signature by use of *asymmetric crypto* system and *hash function*
- Legal recognition of electronic records
- Legal recognition of digital signatures
- Retention of electronic record
- Publication of Official Gazette in electronic form
- Security procedure for electronic records and digital signature
- Licensing and regulation of Certifying Authorities for issuing digital signature certificates
- Functions of Controller
- Appointment of Certifying Authorities and Controller of Certifying Authorities, including recognition of foreign Certifying Authorities
- Controller to act as repository of all digital signature certificates
- Data Protection
- Various types of computer crimes defined and stringent penalties provided under the Act
- Appointment of adjudicating officer for holding inquiries under the Act
- Establishment of Cyber Appellate Tribunal
- Appeal from order of Adjudicating Officer to Cyber Appellate Tribunal and not to any Civil Court
- Appeal from order of Cyber Appellate Tribunal to High Court
- Interception of information from computer
- Special provision for Protected Systems
- Act to apply for offences or contraventions committed outside India
- Network service providers not to be liable in certain cases
- Power of police officers and other officers to enter into any public place and search and arrest without warrant

- Offences by the Companies
- Constitution of Cyber Regulations Advisory Committee who will advice the Central Government and Controller[6]

4.Information Technology (Amendment) Act, 2008

The IT Amendment Bill 2008 has been passed by the Lok Sabha and the Rajya Sabha in the last week of December, 2008. The said Bill aims to make sweeping changes in the existing Indian cyber law, namely the Information Technology Act, 2000. The Information Technology Act, 2000 is India's mother legislation regulating the use of computers, computer systems and computer networks as also data and information in the electronic format. The said legislation has provided for the legality of the electronic format as well as electronic contracts. This legislation has touched varied aspects pertaining to electronic authentication, digital signatures, cyber crimes and liability of network service providers.

From 17th October, 2000, when the Information Technology Act, 2000 came into implementation till date, the said legislation has seen some very interesting cases and challenges, being brought within its ambit. As time passed by, the inadequacies of the said legislation came to the forefront. There were various practical difficulties in the implementation of the said legislation. The inadequacy of the Information Technology Act, 2000 to address some of the emerging phenomena, challenges and cyber crimes, led to voices clamoring for change in the Indian cyber law.

Consequently, the Government of India tabled the Information Technology Amendment Bill, 2006 before both the houses of Parliament in December, 2006, which referred the said amendment bill to the Parliamentary Standing Committee on Information Technology. The Parliamentary Standing Committee examined the proposed amendments in a comprehensive manner and thereafter gave its report and recommendations thereon. The Parliamentary Standing Committee on Information Technology headed by Nikhil Kumar, MP did an excellent job in terms of producing its exhaustive recommendations. These recommendations were noteworthy for their fore vision and clarity of thought process. Way back in 2007, the Standing Committee had recommended that the entire menace of cyber terrorism needs to be addressed with a strong hand. After examining the said recommendations, the Central Government brought the Information Technology Amendment Bill, 2008 in Parliament, which got passed by both the houses of Parliament. Given the magnitude of the amendments, it is indeed strange and amazing that this Bill was passed in an unprecedented hurry, without any discussion in both the houses of the Parliament in the last week of December, 2008.

The IT Amendment Act, 2008 brings about various sweeping changes in the existing Cyber law. While the lawmakers have to be complemented for their appreciable work

removing various deficiencies in the Indian Cyber law and making it technologically neutral, yet it appears that there has been a major mismatch between the expectation of the nation and the resultant effect of the amended legislation. The most bizarre and startling aspect of the new amendments is that these amendments seek to make the Indian cyber law a cyber crime friendly legislation; - a legislation that goes extremely soft on cyber criminals, with a soft heart; a legislation that chooses to encourage cyber criminals by lessening the quantum of punishment accorded to them under the existing law; a legislation that chooses to give far more freedom to cyber criminals than the existing legislation envisages; a legislation which actually paves the way for cyber criminals to wipe out the electronic trails and electronic evidence by granting them bail as a matter of right; a legislation which makes a majority of cyber crimes stipulated under the Information Technology Act, 2000 as bailable offences; a legislation that is likely to pave way for India to become the potential cyber crime capital of the world.

5. New Provisions added through Amendments[7]

- New provision to address technology neutrality from its present "technology specific" form (i.e. 'digital signature' to 'electronic signature')
- New provision to promote e-Governance & other IT application- (i) Delivery of Service; (ii) Outsourcing – Public Private Partnership
- New provision to address electronic contract
- New provision to address data protection and privacy
- Body corporate to implement best security practices
- Multimember Appellate Tribunal
- New provision to address new forms of computer misuse- impersonation; identity theft and e-commerce frauds like phishing; video voyeurism; offensive messages and spam; pornography
- Preservation and retention of data/information
- Revision of existing provisions to empower Central Government to designate agencies and issue direction for interception and safeguards for monitoring and decryption
- Blocking of information for public access
- Monitoring of traffic data and information for cyber security
- New provision for designating agency for protection of Critical Information Infrastructure
- New provision for empowering CERT to call and analyze information relating to breach in cyber space and cyber security
- Revision of existing provisions for prescribing liabilities for intermediaries including cyber cafes; and empowering Central Government to prescribe guidelines to be observed by the service providers for providing services.
- New provision for Examiner of Electronic Evidence
- New modes of encryption

- Punishments for most of offences were reduced from three years to two years.

There are a number of positive developments, as well as many which dismay. Positively, they signal an attempt by the government to create a dynamic policy that is technology neutral. This is exemplified by its embracing the idea of electronic signatures as opposed to digital signatures. But more could have been done on this front.[8] There have also been attempts to deal proactively with the many new challenges that the internet poses.

6. Freedom of Expression

The first amongst these challenges is that of child pornography. It is heartening to see that the provision on child pornography[9] has been drafted with some degree of care. It talks only of sexualized representations of actual children, and does not include fantasy play-acting by adults, etc. From a plain reading of the provision, it is unclear whether drawings depicting children will also be deemed an offence under the provision. Unfortunately, the provision covers everyone who performs the conducts outlined in the provision, including minors. A slight awkwardness is created by the age of "children" being defined in the explanation to the provision as older than the age of sexual consent. So a person who is capable of having sex legally may not record such activity (even for private purposes) until he/she turns eighteen.

Another problem is that the word "transmit" has only been defined for section 66E. The phrase "causes to be transmitted" is used in section 67, 67A, and 67B. That phrase, on the face of it, would include the recipient who initiates a transmission along with the person from whose server the data is sent. While in India, traditionally the person charged with obscenity is the person who produces and distributes the obscene material, and not the consumer of such material. This new amendment might prove to be a change in that position. Section 66A which punishes persons for sending offensive messages is overly broad, and is patently in violation of Article 19(1) (a) of the Constitution. The fact that some information is "grossly offensive" or that it causes "annoyance" or "inconvenience" while being known to be false cannot be a reasons for curbing the freedom of speech unless it is directly related to decency or morality, public order, or defamation (or any of the four other grounds listed in Article 19(2)).

It must be stated here that many argue that John Stuart Mill's harm principle provides a better framework for freedom of expression than Joel Feinberg's offence principle. The latter part of Section 66A(c), which talks of deception, is sufficient to combat spam and phishing, and hence the first half, talking of annoyance or inconvenience is not required. Additionally, it would be beneficial if an explanation could be added to Section 66A(c) to make clear what "origin" means in that section. Because depending on the construction of that word Section 66A(c) can, for instance,

unintentionally prevent organizations from using proxy servers, and may prevent a person from using a sender envelope different form the "from" address in an e-mail (a feature that many e-mail providers like G-mail implement to allow people to send mails from their work account while being logged in to their personal account).

In *Shreya Singhal v. Union of India,* [10] a two-judge bench of the Supreme Court of India in 2015, struck down Section 66-A of the Information Technology Act, 2000, relating to restrictions on online speech as unconstitutional on grounds of violating the freedom of speech guaranteed under Article 19(1)(a) of the Constitution of India. The Court further held that the provision was not saved by virtue of being 'reasonable restrictions' on the freedom of speech under Article 19(2). The case was a watershed moment for online free speech in India.

Furthermore, it may also prevent remailers, tunneling, and other forms of ensuring anonymity online. This does not seem to be what is intended by the legislature, but the section might end up having that effect. This should hence be clarified. Section 69A grants powers to the Central Government to "issue directions for blocking of public access to any information through any computer resource". In English, that would mean that it allows the government to block any website. While necessity or expediency in terms of certain restricted interests is specified, no guidelines have been specified. Those guidelines, per Section 69-A (2), "shall be such as may be prescribed." It has to be ensured that they are prescribed first, before any powers of censorship are granted to anybody. In India, it is clear that any law that gives unguided discretion on an administrative authority to exercise censorship is unreasonable.[11]

Intermediary Liability

The amendment to the provision on intermediary liability[12] while a change in the positive direction, as is seeks to make only the actual violators of the law liable for the offences committed, still isn't wide enough. This exemption is required to be widely worded to encourage innovation and to allow for corporate and public initiatives for sharing of content, including via peer-to-peer technologies. Firstly, the requirement of taking down content upon receiving "actual knowledge" is much too heavy a burden for intermediaries. Such a requirement forces the intermediary to make decisions rather than the appropriate authority.[13]

The intermediary is no position to decide whether a Gauguin painting of Tahitian women is obscene or not, since that requires judicial application of mind. Secondly, that requirement is vitiates the principles of natural justice and freedom of expression because it allows a communication and news medium to be gagged without giving it, or the party communicating through it, any due hearing. It has been held by our courts that a restriction that does not provide the affected persons a right to be heard is procedurally unreasonable. The intermediary loses protection of the act if:

(a) It initiates the transmission;
(b) Selects the receiver of the transmission; and
(c) Selects or modifies the information.

While the first two are required to be classified as true "intermediaries," the third requirement is a bit too widely worded. For instance, an intermediary might automatically inject advertisements in all transmissions, but that modification does not go to the heart of the transmission, or make it responsible for the transmission in any way. Similarly, the intermediary may have a code of conduct, and may regulate transmissions with regard to explicit language (which is easy to judge), but would not have the capability to make judgments regarding fair use of copyrighted materials[14]. So that kind of "selection" should not render the intermediary liable, since misuse of copyright might well be against the intermediary's terms and conditions of use[15].

7. Privacy and surveillance

While the threat of cyber-terrorism might be very real, blanket monitoring of traffic is not the way forward to get results, and is sure to prove counter-productive. It is much easy to find a needle in a small bale of hay rather than in a haystack. Small-scale and targeted monitoring of metadata (called "traffic data") is a much more suitable solution that will actually lead to results, instead of getting information overload through un-channeled monitoring of large quantities of data. If such safeguards are not in place, then the powers might be of suspect constitutionality because of lack of guided exercise of those powers. Very importantly, the government must also follow up on these powers by being transparent about the kinds of monitoring that it does to ensure that the civil and human rights guaranteed by our Constitution are upheld at all times[16].

8.Encryption

The amending law does not really bring about much of a change with respect to encryption, except for expanding the scope of the government's power to order decryption. While earlier, under Section 69, the Controller had powers to order decryption for certain purposes and order 'subscribers' to aid in doing so (with a sentence of up to seven years upon non-compliance), now the government may even call upon intermediaries to help it with decryption.[14] Additionally, Section 118 of the Indian Penal Code has been amended to recognize the use of encryption as a possible means of concealment of a 'design to commit [an] offence punishable with death or imprisonment for life'. The government already controls the strength of permissible encryption by way of the Internet Service Provider licenses, and now has explicitly been granted the power to do so by Section 84A of the Act. However, the government may only prescribe the modes or methods of encryption "for secure use of the electronic medium and for promotion of e-governance and e-commerce." Thus, it is possible to

read that as effectively rendering nugatory the government's efforts to restrict the strength of encryption to 40-bit keys (for symmetric encryption)

Other Penal Provisions

Section 66F (1) (B), defining "cyber terrorism" is much too wide, and includes unauthorized access to information on a computer with a belief that that information may be used to cause injury to decency or morality or defamation, even. While there is no one globally accepted definition of cyber terrorism, it is tough to conceive of slander as a terrorist activity. Another overly broad provision is Section 43, which talks of "diminishing its value or utility" while referring information residing on a computer, is overly broad and is not guided by the statute. Diminishing of the value of information residing on a computer could be done by a number of different acts; even copying of unpublished data by a conscientious whistle blower might, for instance, fall under this clause.

While the statutory interpretation principle of *noscitur a socii* (that the word must be understood by the company it keeps) might be sought to be applied, in this case that doesn't give much direction either. While all offences carrying penalties above three years imprisonment have been made cognizable, they have also been made bailable and lesser offences have been made compoundable. This is a desirable amendment, especially given the very realistic possibility of incorrect imprisonments and frivolous cases that are being registered. Cheating by personation is not defined, and it is not clear whether it refers to cheating as referred to under the Indian Penal Code as conducted by communication devices, or whether it is creating a new category of offence. In the latter case, it is not at all clear whether a restricted meaning will be given to those words by the court such that only cases of phishing are penalized, or whether other forms of anonymous communications or other kinds of disputes in virtual worlds will be brought under the meaning of "personation" and "cheating."

9. Case Studies

- *Sajeesh Krishnan v. State of Kerala*:[17] A petition was filed before the Kerala High Court for release of passport seized at the time of arrest from the custody of the investigating agency. The Court accordingly passed an order for release of the passport of the petitioner. The Court, while deciding the case, briefly mentioned the facts of the case which were relevant to the petition. It stated that the “gist of the accusation is that the accused pursuant to a criminal conspiracy hatched by them made attempts to extort money by black mailing a Minister of the State and for that purpose they have *forged some CD* as if it contained statements purported to have been made by the Minister.” The accused was charged under the provisions of Sections 66-A(b) and 66D of the Information Technology Act, 2000 along with a host of sections under the Indian Penal Code, 1860.[18]

- *Nikhil Chacko Sam v. State of Kerala*:[19] The complainant and the accused (petitioner) were together at Chennai. On 04.09.2009, the petitioner has transmitted photos of the *de facto* complainant and another person depicting them in bad light through internet and thus the petitioner has committed the offence under Section 66-A, IT Act.

- *J.R. Gangwani v. State of Haryana*:[20] A complaint was filed under Section 66-A(c) on the ground of sending e-mails under assumed e-mail addresses to customers of the Company which contained material which maligned the name of the Company which was to be sold as per the orders of the Company Law Board. The Complainant in the case received the e-mails which were redirected from the customers. According to the accused and the petitioner, the e-mail was not directed to the complainant or the company as is required under Section 66-A (c). The High Court held that, "the petitioners are sending these messages to the purchasers of cranes from the company and those purchasers cannot be considered to be the possible buyers of the company. Sending of such e-mails, therefore, is not promoting the sale of the company which is the purpose of the advertisement given in the Economic Times. Such advertisements are, therefore, for the purpose of causing annoyance or inconvenience to the company or to deceive or mislead the addressee about the origin of such messages. These facts, therefore, clearly bring the acts of the petitioners within the purview of section 66A(c) of the Act."

- *Mohammad Amjad v. Sharad Sagar Singh*:[21] In this case, the judge observed that, "Section 66A of Information Technology Act does not refer at all to any 'group' or 'class' of people. The only requirement of Section 66A is that the message which is communicated is grossly offensive in nature or has menacing character."

- *Sandeep Varghese v. State of Kerala*[22] On the basis of a complaint filed by the representative of a Company which was engaged in the business of trading, and distribution of petrochemicals in India and overseas, a case was registered against nine persons, alleging offences under Sections 65, 66, 66 A, C and D of the Information Technology Act, 2000 along with Sections 419 and 420 of Indian Penal Code. The company has a website in the name and style "*wwww.jaypolychem.com*" but, another web-site *www.jayplychem.org* was set up in the internet by the accused. Defamatory and malicious matters about the company and its directors were made available in that website. The first accused and others sent e-mails from fake e-mail accounts of many of the customers, suppliers, Banks etc. to malign the name and image of the company and its directors. The defamation campaign run by all the said persons named above cause immense damage to the name and reputation of the company. The

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

- *Jawaharlal Nehru University MMS Scandal*:[23] In severe shock to prestigious and renowned institute a pornographic MMS clip was apparently made into campus and transmitted outside the university. Some media reports claimed that the two accused students initially tried to extort money from the girl in the video but when they failed the culprits put the video out on mobile phones and even sold C.D in the blue film market. The accused were sentenced under Section 66-E for violation of privacy.

- *Nagpur Congress Leaders MMS Scandal*:[24] On January 5, 2012 Nagpur Police arrested two engineering students one of them a son of Congress leader for harassing a 16 year old girl by circulating an MMS clip of their sexual acts. According to the police the girl was in a relationship with the son of an influential Congress leader in Nagpur district.
- *Cyber Terrorism:* The Mumbai Police have registered a case of "cyber terrorism " – the first in the state since amendment to the Information Technology Act – where a threat e-mail was sent to BSE and NSE on Monday. The IP address of the sender has been traced to Patna in Bihar. The ISP is Sify. The email ID was created just four minutes before the email was sent. "The sender had while creating the new ID given two mobile numbers in the personal details column. Both the numbers belong to a photo frame maker in Patna." The Police have registered forgery for purpose of cheating, criminal intimidation cases under the IPC and cyber terrorism under Section 66- F of the Information Technology Act.

- *Janhit Manch v. The Union of India*:[25] The petition sought a blanket ban on pornographic websites. The NGO had argued that websites displaying sexually explicit content had an adverse influence, leading youth on a delinquent path. The Court observed: "The Act therefore, makes provision for punishment of a person against whom a complaint is filed, if such person commits the offence which falls within the purview of section 67 or 67A as the case may be. Such person can be tried and convicted. For that prosecution will have to establish that an offence has been committed. By the present petition what the petitioner seeks is that this court which is a protector of free speech to the citizens of this country, should interfere and direct the respondents to make a coordinated and sustained efforts to close down the websites as afore stated. Once Parliament in its wisdom has enacted a law and has provided for the punishment for breach of that law any citizen of this country including the Petitioner who is aggrieved against any action on the part of any other person which may amount to an offence has a right to approach the appropriate forum and lodge a complaint upon which the action can be taken if an offence is disclosed. Courts in such

matters, the guardian of the freedom of free speech, and more so a constitutional court should not embark on an exercise to direct State Authorities to monitor websites. If such an exercise is done, then a party aggrieved depending on the sensibilities of persons whose views may differ on what is morally degrading or prurient will be sitting in judgment, even before the aggrieved person can lead his evidence and a competent court decides the issue. The Legislature having enacted the law a person aggrieved may file a complaint. In the light of that we are not inclined to interfere in the exercise of our extra ordinary jurisdiction. If the petitioner comes across any website/s which according to him publishes or transmits any act which amounts to offence under section 67 or 67A of the Information & Technology Act, 2000, it is up to him to file a complaint."

- *Pune Citibank Mphasis Call Center Fraud*: US $ 3,50,000 from accounts of four US customers were dishonestly transferred to bogus accounts. This will give a lot of ammunition to those lobbying against outsourcing in US. It is a case of sourcing engineering. Some employees gained the confidence of the customer and obtained their PIN numbers to commit fraud. They got these under the guise of helping the customers out of difficult situations. Highest security prevails in the call centers in India as they know that they will lose their business. There was not as much of breach of security but of sourcing engineering. The call center employees are checked when they go in and out so they cannot copy down numbers and therefore they could not have noted these down. They must have remembered these numbers, gone out immediately to a cyber café and accessed the Citibank accounts of the customers. All accounts were opened in Pune and the customers complained that the money from their accounts was transferred to Pune accounts and that is how the criminals were traced. Police has been able to prove the honesty of the call center and has frozen the accounts where the money was transferred.

- *Avnish Bajaj v State (N.C.T.) of Delhi* (*bazee.com case*):[27] CEO of Bazee.com was arrested in December 2004 because a CD with objectionable material was being sold on the website. The CD was also being sold in the markets in Delhi. The Police got into action. The CEO was later released on bail. This opened up the question as to what kind of distinction do we draw between Internet Service Provider and Content Provider. The burden rests on the accused that he was the Service Provider and not the Content Provider. It also raises a lot of issues regarding how the police should handle the cyber crime cases and a lot of education is required.

- *State of Tamil Nadu v. Suhas Kutti*:[28] The accused, on 7.2.2004 evening at Cyber Café Hello World Centre, Mumbai having an I.P.61.11.10.99, with an intention of harming the reputation of the Complainant, Ms. R, created user id in the name of her and composed an obscene message intending that such document shall be

used for posting in different obscene Yahoo Group, with the intention to make others to believe that the document was made by her, so that the persons seeing the obscene message would send offending calls to her. Thereby the accused have committed offences u/s 469 & 509 IPC and 67 of I.T. Act. The obscene message carried her Office phone numbers and her e-mail I.D. The house Phone number was wrongly given. The said obscene messages have been sent through Yahoo website to 5 sex groups. On seeing the said messages, several persons sent the responsive message and many persons tried to contact her over phone. The accused was convicted and sentenced to undergo rigorous imprisonment for 2 years u/s 469 IPC, and to pay a fine. This was the first case in India where a conviction was handed down in connection with the posting of obscene messages on the internet under the controversial section 67 of the Information Technology Act, 2000.

- *The Bank NSP Case:* The Bank NSP case is the one where a management trainee of the bank was engaged to be married. The couple exchanged many emails using the company computers. After some time the two broke up and the girl created fraudulent email ids such as "Indian bar associations" and sent emails to the boy's foreign clients. She used the banks computer to do this. The boy's company lost a large number of clients and took the bank to court. The bank was held liable for the emails sent using the bank's system.

- *SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra*:[29] In India's first case of cyber defamation, a Court of Delhi assumed jurisdiction over a matter where a corporate's reputation was being defamed through emails; and passed an important ex-parte injunction. In this case, the defendant being an employ of the plaintiff company started sending derogatory, defamatory, obscene, vulgar, filthy and abusive emails to his employers as also to different subsidiaries of the said company all over the world with the aim to defame the company and its Managing Director. The plaintiff filed a suit for permanent injunction restraining the defendant from doing his illegal acts of sending derogatory e-mails to the plaintiff. On behalf of the plaintiffs it was contended that the emails sent by the defendant were distinctly obscene, vulgar, abusive, intimidating, humiliating and defamatory in nature. Counsel further argued that the aim of sending the said emails was to malign the high reputation of the plaintiffs all over India and the world. He further contended that the acts of the defendant in sending the emails had resulted in invasion of legal rights of the plaintiffs. Further the defendant is under a duty not to send the aforesaid emails. It is pertinent to note that after the plaintiff company discovered the said employ could be indulging in the matter of sending abusive emails, the plaintiff terminated the services of the defendant. After hearing detailed arguments of the plaintiff, the Delhi High Court passed an *ex-parte* interim injunction observing that a *prima facie* case had been made out

by the plaintiff. Consequently, the Delhi High Court restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails either to the plaintiffs or to its sister subsidiaries all over the world including their Managing Directors and their Sales and Marketing departments.

- *Parliament Attack Case*: Bureau of Police Research and Development at Hyderabad had handled some of the top cyber cases, including analyzing and retrieving information from the laptop recovered from terrorist, who attacked Parliament. The laptop which was seized from the two terrorists, who were gunned down when Parliament was under siege on December 13th 2001, was sent to Computer Forensics Division of BPRD after computer experts at Delhi failed to trace much out of its contents. The laptop contained several evidences that confirmed of the two terrorists' motives, namely the sticker of the Ministry of Home that they had made on the laptop and pasted on their ambassador car to gain entry into Parliament House and the fake ID card that one of the two terrorists was carrying with a Government of India emblem and seal. The emblems (of the three lions) were carefully scanned and the seal was also craftily made along with residential address of Jammu and Kashmir. But careful detection proved that it was all forged and made on the laptop.

- *Andhra Pradesh Tax Case*: Dubious tactics of a prominent businessman from Andhra Pradesh was exposed after officials of the department got hold of computers used by the accused person. The owner of a plastics firm was arrested and Rs 22 crore cash was recovered from his house by sleuths of the Vigilance Department. They sought an explanation from him regarding the unaccounted cash within 10 days. The accused person submitted 6,000 vouchers to prove the legitimacy of trade and thought his offence would go undetected but after careful scrutiny of vouchers and contents of his computers it revealed that all of them were made after the raids were conducted. It later revealed that the accused was running five businesses under the guise of one company and used fake and computerized vouchers to show sales records and save tax.
- *Sony.sambandh.com case*:[30] A complaint was filed by Sony India Private Ltd, which runs a website called *www.sonysambandh.com*, targeting Non Resident Indians. The website enables NRIs to send Sony products to their friends and relatives in India after they pay for it online. The company undertakes to deliver the products to the concerned recipients. In May 2002, someone logged onto the website under the identity of Barbara Campa and ordered a Sony Color Television set and a cordless head phone. She gave her credit card number for payment and requested that the products be delivered to Arif Azim in Noida. The payment was duly cleared by the credit card agency and the transaction processed. After following the relevant procedures of due diligence and checking, the company delivered the items to Arif Azim. At the time of delivery, the

company took digital photographs showing the delivery being accepted by Arif Azim. The transaction closed at that, but after one and a half months the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase. The company lodged a complaint for online cheating at the Central Bureau of Investigation which registered a case under Sections 418, 419 and 420 of the Indian Penal Code. The matter was investigated into and Arif Azim was arrested. Investigations revealed that Arif Azim, while working at a call centre in Noida gained access to the credit card number of an American national which he misused on the company's site. The CBI recovered the color television and the cordless head phone. In this matter, the CBI had evidence to prove their case and so the accused admitted his guilt. The court convicted Arif Azim under Sections 418, 419 and 420 of the Indian Penal Code — this being the first time that a cybercrime has been convicted. The court, however, felt that as the accused was a young boy of 24 years and a first-time convict, a lenient view needed to be taken. The court therefore released the accused on probation for one year. The judgment is of immense significance for the entire nation. Besides being the first conviction in a cybercrime matter, it has shown that the Indian Penal Code can be effectively applied to certain categories of cyber crimes which are not covered under the Information Technology Act 2000. Secondly, a judgment of this sort sends out a clear message to all that the law cannot be taken for a ride.

- *Nasscom v. Ajay Sood*: The Delhi High Court declared `phishing' on the internet to be an illegal act, entailing an injunction and recovery of damages. Elaborating on the concept of 'phishing', in order to lay down a precedent in India, the court stated that it is a form of internet fraud where a person pretends to be a legitimate association, such as a bank or an insurance company in order to extract personal data from a customer such as access codes, passwords, etc. Personal data so collected by misrepresenting the identity of the legitimate party is commonly used for the collecting party's advantage. Court also stated, by way of an example, that typical phishing scams involve persons who pretend to represent online banks and siphon cash from e-banking accounts after conning consumers into handing over confidential banking details. The Delhi HC stated that even though there is no specific legislation in India to penalize phishing, it held phishing to be an illegal act by defining it under Indian law as "a misrepresentation made in the course of trade leading to confusion as to the source and origin of the e-mail causing immense harm not only to the consumer but even to the person whose name, identity or password is misused." The court held the act of phishing as passing off and tarnishing the plaintiff's image. The plaintiff in this case was the National Association of Software and Service Companies (Nasscom), India's premier software association. The defendants were operating a placement agency involved in head-hunting and recruitment. In order to obtain personal data, which they could use for purposes of headhunting,

the defendants composed and sent e-mails to third parties in the name of Nasscom. The court recognized the trademark rights of the plaintiff and passed an ex-parte ad interim injunction restraining the defendants from using the trade name or any other name deceptively similar to Nasscom. The court further restrained the defendants from holding themselves out as being associates or a part of Nasscom. The court appointed a commission to conduct a search at the defendants' premises. Two hard disks of the computers from which the fraudulent e-mails were sent by the defendants to various parties were taken into custody by the local commissioner appointed by the court. The offending e-mails were then downloaded from the hard disks and presented as evidence in court. During the progress of the case, it became clear that the defendants in whose names the offending emails were sent were fictitious identities created by an employee on defendants' instructions, to avoid recognition and legal action. On discovery of this fraudulent act, the fictitious names were deleted from the array of parties as defendants in the case. Subsequently, the defendants admitted their illegal acts and the parties settled the matter through the recording of a compromise in the suit proceedings. According to the terms of compromise, the defendants agreed to pay a sum of Rs1.6 million to the plaintiff as damages for violation of the plaintiff's trademark rights. The court also ordered the hard disks seized from the defendants' premises to be handed over to the plaintiff who would be the owner of the hard disks. This case achieves clear milestones: It brings the act of "phishing" into the ambit of Indian laws even in the absence of specific legislation; It clears the misconception that there is no "damages culture" in India for violation of IP rights; This case reaffirms IP owners' faith in the Indian judicial system's ability and willingness to protect intangible property rights and send a strong message to IP owners that they can do business in India without sacrificing their IP rights.

- *Google India Pvt. Ltd., v. Visaka Industries Limited:* It was contended by the senior counsel appearing for the petitioner that the actions of intermediaries such as Google Inc., which is a service provider providing platform for end users to upload content, does not amount to publication in law and consequently the question of holding such intermediaries liable for defamation does not arise. Senior Counsel appearing for the petitioner placed reliance on Section 79 of the Information Technology Act, 2000 in support of this contention. Section 79 which occurs in Chapter XII of the Act originally as it stood enacted in the year 2000 reads as follows: Network service providers not to be liable in certain cases: For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made there under for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention. Explanation: For the purposes of

this section, (a) "network service provider" means an intermediary; (b) "third party information" means any information dealt with by a network service provider in his capacity as an intermediary." The said provision exempts network service providers from liability under the Act, rules or regulations made there under for any third party information or data made available by him. It did not exempt a network service provider from liability much less criminal liability for the offences under other laws or more particularly under the Indian Penal Code. Further, the above provision exempts network service provider from liability, only on proof that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention. Proof in that regard can be let in by way of leading evidence by the accused. (1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him. (2) The provisions of sub-section (1) shall apply if- (a) the functions of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or (b) the intermediary does not- (i) initiate the transmission, (ii) select the receiver of the transmission, and (iii) select or modify the information contained in the transmission; (c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf. (3) The provisions of Sub-section(1) shall not apply if- (a) The intermediary has conspired or abetted or aided or induces whether by threats or promise or otherwise in the commission of the unlawful act; (b) upon receiving actual knowledge, or on being notified by information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner. Explanation.- For the purposes of this section, the expression "third party information" means any information dealt with an intermediary in his capacity as an intermediary."

- *Microsoft Corporation v. Yogesh Papat*:[31] This case concerns the infringement of copyright in software and notably the interpretation of Sections 51 and 55 of the Copyright Act 1957. The Microsoft Corporation, the registered proprietor of the trademark MICROSOFT, requested a permanent injunction restraining the defendant, its directors and agents from copying, selling, offering for sale, distributing or issuing to the public counterfeit or unlicensed versions of Microsoft's software program in any manner that amounts to infringement of Microsoft's copyright in the computer programs, related manuals and Microsoft's registered trademarks. Microsoft also requested that the defendant be prevented

from selling and distributing any product to which the trademark MICROSOFT or any variants of this trademark have been applied. The defendant did not appear before the court, so the proceedings took place ex parte. The court eventually ruled against the defendant, who was downloading Microsoft software onto the hard drives of computers that it then sold, without a license or permission to do so from Microsoft. Decision The court approached each piece of evidence in turn and, based on the assumption that 100 computers were sold each year and on the evidence of the software's popularity, held that Microsoft had suffered a total profit loss of Rs1.98 million, plus interest at 9% from the date of the decree until the date of payment. The court, quoting an observation by Justice Laddie in the High Court of England and Wales in *Microsoft Corporation v. Electrowide Ltd*,[32] held that the defendant's actions "constituted a general threat to infringe the copyright in the class of software." Nandrajog J., who presided in this case, stated that: "It stands established that the defendant has infringed the plaintiff's copyright by making illicit copies of the operating systems software by openly copying whatever operating system is currently saleable."

10. Summary

The challenges faced by cyber laws are vast due to geographical hurdles, cultural patterns and land laws governing one's particular land. Easy access to cyberspace is one of the main reasons for the growth of cyber crime thereby threat to the national security of the country. There exists a dearth of adequate laws. According to NASSCOM, there is extremely low rate of conviction of cyber crime in India. The statistics show that 1600 have been arrested against 3682, where the conviction is shocking 7 of which 3 are significant. To look into more detail the number of crime has gone up by tenfold. Such a rise in the crime is due to low rate of conviction rate. In the year 2007, the arrests made were 154 while in the following year there was 178. In the years 2009 and 2010, the numbers of persons arrested were 288 and 799 and in 2011, it was 1,184. This shows clearly a huge rise in the number of arrests but yet a single digit conviction rate. A further record also show that 217,288, 420,966 and 1,791 cyber crime cases were registered under IT Act, 2000 during the years 2007, 2008, 2009, 2010 and 2011.

In India, the government has taken steps in the framing of The National Cyber Security Policy. This policy proposes to:

(a) Facilitate collaboration between government agencies and private cyber security solutions developers in order to optimize and protect critical government initiatives
(b) The policy is a road map for strengthening cyber security as it will secure a computing framework that will inspire consumer confidence for electronic transaction.

(c) At the macro level the policy will facilitate cyber security intelligence that will form an integral component to anticipate attacks and quickly adopt counter measures.

The Central and the State Government have been authorized to issue directions for interception or monitoring or decryption of any information through any computer resource. Both the governments, in the interest of sovereignty or integrity of India, defense of India, security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, may intercept, monitor or decrypt or cause to intercepted, monitored or decrypted any information generated, transmitted received or stored in any computer resource. They can block public access to any information through any computer resource. Dream to keep the society crime-fee will remain a dream in India as there should be constant endeavor for the legislation to keep in pace with the fast pace in crimes. Especially in a society that is dependent more and more on technology, crime based and electronic offences are bound to increase and the law makers have to go the extra mile keeping in pace to the fraudsters as technology is always a double-edged sword and can be used for both the purposes – good or bad.

11. Reference

1. Talat Fatima, *Cybercrim*e (Eastern Book Company, Lucknow, 2011), p. 89
2. Suresh T. Vishwanathan, *The Criminal Aspect in Cyber Law in The Indian Cyber Law* (Bharat Law House, 2001), p.7
3. Articles 2-10
4. A/RES/51/162, dated the 30th January, 1997
5. For ‘digital certificates’ as per Information Technology Act, 2000 and since replaced by ‘electronic signatures’ in the Information Technology Amendment Act, 2008.
6. Jitender K Malik, Dr. Sanjaya Choudhury A Brief review on Cyber Crime - Growth and Evolution, Pramana Research Journal, 2019, 9(3), 242- 278.
7. Jitender Kumar Malik and Sanjaya Choudhury, PolicyXZ. International Journal of Recent Scientific Research, Vol. 9, issue 12(A) , December, 2018, pp. 29811-29814
8. Jitender k malik, cyber-crimes- policy in India, International Research Journal of Human Resources and Social Sciences, Volume 5, Issue 04, April 2018, 554-565.
9. Jitender Kumar Malik and Sanjaya Choudhury, PolicyXZ. International Journal of Recent Scientific Research, Vol. 9, issue 12(A) , December, 2018, pp. 29811-29814

10. Jitender k malik, cyber-crimes- policy in India, International Research Journal of Human Resources and Social Sciences, Volume 5, Issue 04, April 2018, 554-565.
11. J Malik, Dr. Sanjaya Choudhury, Journal of Information and Computational Science, Volume 9 Issue 12, 2019, 432-447.
12. For instance, section 76 of the Act still talks of floppy disks A
13. IR 2015 SC 1523.
14. *Virendra v. State of Punjab*, AIR 1957 SC 896
15. Section 79
16. *In re Venugopal*, AIR 1954 Mad 901
17. Kerala High Court, decided on June 5, 2012
18. Sections 120B (Criminal conspiracy), 419 (Cheating by personation), 511 (Punishment for attempting to commit offences punishable with imprisonment for life or other imprisonment), 420 (Cheating and dishonestly inducing delivery of property), 468 (Forgery for purpose of cheating), 469 (Forgery for purpose of harming), 201 (Causing disappearance of evidence of offence, or giving false information to screen offender) read with 34 (joint liability).
19. Kerala High Court, decided on July 9, 2012
20. Punjab & Haryana High Court, decided on October 15, 2012.
21. Criminal Revision No. 72/2011 (Saket Court, Delhi).
22. Kerala High Court, Bail Application No. 2003 of 201; decision dated 11th June, 2010.
23. MMS Scandal Hits JNU" *Hindustan Times* (February 8, 2011)
24. *One India News* (January 5, 2012).
25. Original Suit No. 1279 of 2001 (Delhi HC)
26. *Afzal Guru v. State*, Criminal Appeals 376-378/2004.
27. Jitender K. malik and Sanjaya Choudhury, Cyber Space- Evolution & Growth. East African Scholars Journal of education, Humanities and Literature, Vol 2(3), 2019, 170-190.
28. Jitender Kumar Malik and Sanjaya Choudhury, A BRIEF REVIEW ON CYBER CRIME -GROWTH AND EVOLUTION. Pramana Research Journal, Volume 9, Issue 3,2019, 242.
29. Jitender Kumar Malik and Sanjaya Choudhury, Policy Considerations In India Against Cyber Crime. International Journal of Recent Scientific Research,Vol. 9, Issue, 12(A), December, 2018, 29811-29814.

30. Jitender Kumar Malik and Sanjaya Choudhury, The Criminals In A Cyber Environment Using Computer Networks. International Journal Of Current Innovation Research, Vol 4, Issue 12 (A) , Dec 2018, 1416-1422.

31. Jitender k malik and Sanjaya Choudhury, Cyber Crimes- Policy In India, International Research Journal of Human Resources and Social Sciences, Volume 5,Issue 04, April 2018, 554-565.