HUMAN RIGHTS AND CYBERSPACE: USE AND MISUSE

Mr. Karra Kameswara Rao*

Abstract

The main focus of this paper is to enlighten not only the academicians but also the non tech savvy laymen to have first-hand information about latest electronic gadgets i.e. internet, cell phones, laptops, etc. and their linkage with human rights across the world. This paper acts like a litmus test to check the use and misuse of cyber space, the new technical name doing wonders in many a field.

The internet has now become all encompassing; it touches the lives of every human being. We now a days, undermine the benefits of internet, however its anonymous nature allows miscreants to indulge in various cybercrimes. As is known well a kitchen knife can be used for cutting vegetables to prepare a good meal but at the same time, the same knife can also be misused to kill a person. Similarly, the cyberspace can also be used and misused.

The only difference between a traditional crime and a cybercrime is that the cybercrime involves in a crime related to computers.

Here is an illustration:

Traditional theft: A thief breaks into X's house and steals an object kept in the house.

Hacking: A cyber-criminal/Hacker sitting in his own house with his computer in hand, hacks the computer of X and steals the data saved in X's computer without physically touching the computer or entering into X's house. Cyber cases related to interception and snooping are increasing at an alarming rate. To curb such crimes cyber laws are being amended to suit the demands of the users. The government at the center and the states as well, are well seized of the matter to tackle the trickish issue in all seriousness. One may wonder what the human rights are to do with or what the nexus is between human rights and cyber space use and misuse. The answer to this query is simply in the affirmative and there is no second thought about it.

* Sr. Assistant Professor, Mahatma Gandhi Law College, Hyderabad.

As an example let us take Intellectual property in cyber space. Internet is one such a threat, which has captured the physical market place and has converted it into virtual market place.

Therefore, it is the duty of the Intellectual Property Right (I.P.R) owner to invalidate and reduce such mala fide acts of criminals by taking proactive measures. Indeed, it is alarming to note a sea change in malfunctioning of cyber space. The recent malware named Uroburos/Snake, is an example of growing cyber espionage and cyber warfare. Stealing of sensitive information is the new trend.

Digital signatures are mostly used for software distribution, financial transactions and in other cases where there is a risk of forgery.

The Indian Parliament passed the Information Technology Act 2000 and amended in 2008 on the United Nations Commissions on International Trade Law (U.N.C.I.T.R.A.L) model Law. The law defines the offences in a detailed manner along with penalties for each category of offences. Thus cyber laws are the safe savior to combat cyber-crime.

Human Rights in the digital age are being contested very openly today. The text of World Summit on the Information Society (W.S.I.S) (Convened on December 2003) Declaration of principles exposes a common vision of the information society, particularly with respect to Human Rights.

This also examines the conflicts of law in civilians (mainly tort laws and laws on the protection of rights of the personality as well as intellectual property and criminal matters.

Keywords: Cyber Space, Cyber Crime, Hacking, Intellectual Property Rights, Human Rights

Introduction

Answers to the following queries will certainly enable us to have refreshing thoughts about the theme of the seminar and better appreciate the efforts of the government, social organizations, institutions and also individuals

1. How does the cyber space overshadow the Human Rights in the light of ongoing increase in the cyber-crime rate?
2. Why don't the law makers take cognizance of the violations of Human rights as enshrined in the universal declaration

of Human Rights (1948) and suitably modify the corrective measures?

3. Is there no scope to tighten the cyber laws, take stringent action against the defaulters and bring relief and succor to the innocent and gullible victims?

4. Is it not the need of the hour that voluntary organizations across the world to wake up and initiate steps in line with the consumer protection act or any other redressal measures provided under the law to put an end to this menace that spread like a cancerous disease?

"DUNIYA MUTTI MEIN" is the buzz word across the world, with the onset of internet. The internet has now become all-encompassing; it touches the lives of every human being. We cannot undermine the benefits of internet; however, its anonymous nature allows miscreants to indulge in various cyber-crimes.

Cyber space can be defined as an intricate environment that involves interactions between people, software and services.

Cyber security denotes the technologies and procedures intended to safeguard computers, networks and data from unlawful admittance weaknesses and attacks transported through the internet by cyber delinquents.

The Ministry of Communications and Information Technology under the Government of India provides a strategy outline called "The National Cyber Security Policy". The purpose of this government body is to protect the public and private infrastructure from cyber-attacks.

Malicious use of information technology can easily be concealed. It is difficult to determine the origin or the identity of the criminal, the motives for disruption can be anything such as:

- Simply demonstrating technical prowess
- Theft of money or information
- Extension of state conflict etc.

Intellectual property refers to creations of the human mind, for example: a story, a song, a painting, a design, a program etc. The facets of intellectual property that relates to cyber space are covered by cyber law namely:

- Copy right Law
- Trademark Law
- Semiconductor Law
- Patent Law

Data protection and privacy laws aim to achieve a fair balance between the Piracy rights of individual and the interests of data controllers such as Banks, Hospitals, Electronic Mails service providers etc.

The appointment of adjudicating officers to decide the fate of multi-crore cyber-crime cases in India was the result of the Public Interest Litigation (P.I.L) filed by the students of Asian School of Cyber Laws (A.S.C.L).

The Indian Penal Code (as amended by the I.T. Act) penalises several cyber-crimes. These include forgery of electronic records, cyber frauds, destroying electronic evidence etc.

Digital evidence is to be collected and proven in the court of law as per the provisions of the Indian Evidence Act (as amended by the I.T. Act).

Every new invention in the field of technology experiences a variety of threats. Internet is one such threat, which has captured the physical market place and has converted it into a virtual market place. The need of the hour is to initiate some stringent strategies in order to design and implement a secure cyber space. This paper is meant to explain the major strategies employed to ensure the cyber securities which are as follows:

- Creating a secure cyber ecosystem
- Creating a mechanism for I.T security
- Security e-governance service
- Protecting critical information infrastructure

Fortunately, the Reserve Bank of India has implemented security and risk mitigation measures for card transactions in India enforceable from 01-10-2013. It has put the responsibility of ensuring secured card transactions upon bank rather than on the customers.

Human rights in the digital age are being contested very openly today. Article 19 of the Universal Declaration of Human Rights is Central to the information society. Every one everywhere should have the opportunity to participate and no one should be excluded from the benefits that the information society offers.

The second part of the paper deals with the traditional human rights relevant to cyber space and to the broader concept of "right to access, cyber space, as well as the uncertainties derived from the fact that a plurality of state and non-state actors may limit and interfere with human rights in cyber space.

The current social and democratic functions of cyber space are barely reflected in current human rights instruments and modern constitution.

Human Rights and Cyber Space

Day in and day out we find human rights violations and privacy of an individual is at stake with the recent advancements in the cyber space. A sincere effort is made to focus on the asserted boundlessness" of cyber space in order to examine how and to what extent the activities are centered round. Before we go deep into the subject, it is appropriate and necessary to understand the meaning and scope of cyber space.

What is Cyber Law?

Cyber Law is the law governing cyberspace. Cyber law is a very wide term and includes computers, networks, software, data storage devices (such as hard discs, USB (universal serial bus controllers) discs, pen drives, flash drives etc.); the internet, websites, electronic mails and even electronic devices such as cellular phones, ATM (Automated Teller Machines) etc.

Cyber law deals with the following:

1. Cyber Crimes
2. Electronic and Digital Signatures
3. Intellectual Property
4. Data protection and Privacy

Cyber-crimes: These crimes are unlawful acts where the computer is used either as a tool or a target or both.

Electronic Signatures: These are used to authenticate electronic records. Digital signatures are one type of electronic signature. Digital signatures satisfy three major requirements -finger authentication (impression-biometric), message authentication and message integrity.

Intellectual Property: Intellectual Property refers to creations of the human mind, eg: a story, a song, a design, a program etc. The facets of intellectual property that relate to cyber space are covered by cyber law.

Data Protection and Privacy: Laws aim to achieve a fair balance between the privacy of the individual and the interests of data controllers such as banks, hospitals, electronic mail service providers etc.

Why to Study Cyber Law?

The following are the reasons:

1. Cyber space is an intangible dimension that is impossible to govern and regulate using conventional law.
2. Cyber space has complete disrespect for jurisdictional boundaries. For example: - A person in India could break into a bank's electronic vault hosted on a computer in U.S.A and transfer millions of dollars into another bank in Switzerland, all within minutes. What he requires is a laptop, computer and a cellular phone.
3. Cyber space offers enormous potential for anonymity to its members.
4. Electronic information is the main object of cyber-crime.
5. Cyber space is the root cause for piracy by which a software source code worth crores of rupees can be pirated across the globe within no time, once it is released.
6. Theft corporeal information is made very easy through cyber space, where "original" information, remains intact in the hands of the "real owner" but tactfully the whole information gets stolen.

The Indian Penal Code (as amended by the I.T. Act) penalizes several crimes, which include forgery of electronic records, cyber frauds, destruction of electronic evidence act.

In an ordinary parlance a computer has the following characteristics:

1. It is a high speed data processing device or a system or a machine.
2. It is electronic, magnetic, optical device.
3. It performs logical, arithmetic and memory functions.
4. All these functions are carried out by manipulations of electronic, magnetic or optical impulses.

According to American Law electronic means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

A data processing device or System is a mechanism that can perform pre-defined operations upon information. The following are some functions:

- Saving information on a hard disk
- Logging on to the internet
- Retrieving stored information
- Calculating mathematical formulae

There is a classic case of Karnataka High Court, which held that ATM's are not computers but electronic devices under the Karnataka's Sales Tax Act, 1957.

Diebold Systems Private Limited v. *Commissioner of Commercial Taxes* [1]

Diebold Systems Private Limited (a manufacturer and supplier of Automated Teller Machines) had sought a clarification from the Advance Ruling Authority (A.R.A) in Karnataka on the rate of tax applicable under the Karnataka Sales Tax Act 1957 on sale of ATMs. The Majority view of the A.R.A was to classify ATMs as Computer terminals" liable for 4% basic tax. The chairman of the A.R.A opined that ATMs as "Electronic Goods" as such would attract 12% basic tax.

The Commissioner of Commercial Taxes dissented with the order of the chairman and held that ATMs cannot be classified as Computer terminals.

The Karnataka High Court held that ATM is not a computer by itself and it is connected to a computer which performs the tasks of ATM. The Computer is connected electronically to many ATM's that may be located at some distances from the computer.

What is Data?

1. A representation of information knowledge, facts, concepts or instructions.
2. Prepared or being prepared in a formalised manner.
3. Processed, being processed or sought to be processed in a computer.

Illustration:

Latha is typing a document on her computer, the moment she pressed keys on her keyboard the corresponding alphabets are

[1] ILR 2005 KAR 2210, (2006) 144 STC 59(KAR).

shown on her screen. But in the background, some parts of the document are stored in the R.A.M (Random Access Memory) of her computer (being processed) while other parts are stored on the hard task (processed). At any given instant some information would be passing from her keyboard to the computer (sought to be processed).

Having thus discussed about the technical aspects of cyber-crime, cyber space, data processing systems, which give a bird's eye view of the sub theme it would be more appropriate and apt to deal with the Human Rights aspects to clinch the issue threadbare and focus on the merits of the theme for better understanding.

Human Rights

The internet has been in existence since 1960's and the World Wide Web (WWW) since 1990's[2]. Cyber space however remains a relatively new terrain in terms of the questions it raises about human rights and responsibilities. The International Telecommunications Union estimates that almost 40% of the world's population and over 76% of people in developed countries are now internet users.[3] Government, business and organizations in civil society are increasingly using cyber space platforms in the communication of information and delivery of services. Accordingly, the internet has become a major vehicle for the exercise of the right to freedom of expression and information. The International Covenant on Civil and Political Rights (I.C.C.P.R)[4] states (in Article 19(2)) Freedom of opinion and expression.

Everyone shall have the right to freedom of expression, this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art or through any other media of his choice.

The United Nations Human Rights Commission (UNHRC) has provided extensive commentary on this article in General Comment Number 3.[5] The Human Rights Commission has stated that the freedom of expression and information under Article 19 of

---

2 *See* Connolly D., *A Little History of the WWW*, *available at* http://www.w.org/history.html 2013.
3 http:// www.itu.intlenl/ITU-27-08-2013.
4 http://www.austlii.edu.au/treaties.27-08-2013.
5 UNDOCLPR/C/GC/34(2011) viewed 27-08-2013

the ICCPR include the freedom to receive and communicate information, ideas and opinions through the internet.[6]

Article 19(3) provides that:

The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as provided by a law and are necessary:

a) For respect of the rights or reputations of others
b) For the protection of national security or public order (order public), or public health or morals.

This means that (like many other rights) the right to freedom of information must be balanced with other rights[7]. The United Nations Human Rights Commission has stated that "The same rights that people have offline must also be protected online" (mentioning in particular freedom of expression)

Laws seeking to balance rights and responsibilities often distinguish between public and private conduct. The rapid development of the internet in terms of its use in daily life has blurred these lines. These days the people across the world are so habituated to the internet activities that it has become a part of their life. Indeed, it is not at all an exaggeration to say the least they have become slaves, so much to say, even dependent upon "private communications" (i.e. always connected to friends; family, social groups as in a virtual world).

In this context a question is pertinent.

How does cyber space intervene in the private communications domain?

Will not cyber space act as a barrier in the sphere of personal life of privacy?

Now the question arises to position of "Public Life":

How do the Anti-discrimination laws identify and applicable to specific areas of "Public Life"?

(For example: employment, accommodation, education, provision of goods and services)

---

6 HRC.GC. No. 34, note 4, para 12.
7 http://ap.ohchr.org/documents/dpage 27-08-2013.

The internet use undoubtedly has rapidly exposed the user in these areas and much can be said on either side. Again an interesting question does arise, as to how can rules in anti-discrimination or other laws be enforced in relation to conduct on the internet where there are questions about the location, place, time of the act complained of occurred?

The main focus of this paper is that the creation of the internet or cyber space has not unlashed a set of "New behaviours" – on the other hand, it to help a greater extent reproduces or recasts the pre-existing behaviours or attitudes within an online medium. Now it has to be seen and judged what could be the impact on these changes and relevance of Human Rights under these circumstances.

Constitutional Provisions and Cyber Space

Comparison between Universal Declaration of Human Rights, 1948 and Fundamental Rights Part-III of Indian Constitution

Indian Constitution	**Universal Declaration of Human Rights,1948**
Article 14: The state shall not deny to any person equality before the law.	Article 1: All are equal before the law and so on…….
Article 19: Freedom of speech, assembly, association etc.	Article 19: Everyone has a right to freedom of opinion and expression
Article 21: No person shall be deprived of his life or personal liberty except according to procedure established by law	Article 3: Everyone has the right to life, liberty and security of person
Article 23(1): Traffic in human beings and other similar forms of forced labour are prohibited.	Article 4: No one shall be held in slavery or servitude ….
Article 32(1): The Right to move the Supreme Court …. For enforcement of Fundamental Rights	Article 8: Everyone has the right to an effective remedy……. For violating fundamental rights

In the Indian Constitution, the justiciable human rights broadly speaking, were included in part-III, while the non-justiciable

social and economic rights were set forth in part-IV in the Directive Principles of State Policy[8]

The Directive Principles of State Policy are mentioned in part-IV of the Constitution of India covering Articles from 36 to 51. The Directive Principles of State Policy are not enforceable. Universal Declaration of Human Rights speaks of similar rights.

A serious effort and great care is taken in this paper to highlight three issues namely:

1. Freedom of expression and internet censorship
2. Effective responses to racism, sexism, sexual harassment and homophobia on the internet
3. Rights to access the internet

Freedom of Expression and the Internet Censorship

The internet has opened up new possibilities, avenues, and channels for the realization of the right to freedom of expression. This is certainly because of the internet's unique characteristics including its speed, worldwide reach and importantly the aspect of anonymity.[9]

These distinctive features have enabled individuals to use the internet to disseminate information in "real time" and to mobilise people[10]. The United Nation's Special Rapporteur on the promotion and protection of the Right to Freedom of opinion and Expression (Special Rapporteur) asserts that:

"Unlike any other medium the internet facilitated the ability of individuals to seek, receive and impart information and ideas of all kinds instantaneously and inexpensively across national borders. By vastly expanding the capacity of individuals to enjoy their right to freedom of opinion and expression, which is an "enabler" of other human rights, the internet boosts economic, social and political development and contributes to the progress of human kind as a whole."[11]

---

8 GEORGE PATHANMACKEL, THE CONSTITUTION OF INDIA-A PHILOSOPHICAL REVIEW 177 (Delhi: Media House, 2003).
9 http://www.ohchr.org/EN/issues.27-08-2013.
10 *Id.* at 7.
11 *Id.* at 19.

However, the special rapporteur acknowledges "like all technological inventions, the internet can be misused to cause harm to others."[12]

Permissbale Limitations of I.C.C.P.R

Right to Freedom of Expression

Article 19(3) of the ICCPR permits limitations on the rights recognised in Article 19(2) but those limitations must be:

1. Provided by law and
2. Necessary for respect of the rights or reputations of others, for protection of national security, public order or public health or morals

Permissible purposes:

- **a)** Respect for the rights or reputation of others
- **b)** Freedom from discrimination
- **c)** Freedom from cruel, inhuman and degrading treatment
- **d)** right to privacy, family, home, correspondence honour and reputation, Article 17 of ICCPR
- **e)** Public morals

Current issues of Internet Censorship

(Australia Media Study)

The Australian media has increasingly reported on a wide range of issues relating to forms of internet censorship, including tracing, internet-based child pornography rings, courts ordering the removal of "Facebook" hate pages involving suspects of crimes, or calls to regulate bullying or offensive behaviours.

Cyber Bullying

Perhaps the most well-known "Cyber" form of offensive behavior is "Cyber Bullying". Cyber bullying is defined as a person (or a group of people) using technology to repeatedly and intentionally use negative words and / or actions against a person which causes distress and risks that person's well-being.[13]

Impact of Cyber Bullying:

The following are the impacts of cyber bullying:

---

12 *Id.*

13 http://www.ncab.org.au,28-08-2013.

- The right to the highest attainable standard of physical and mental health.[14] Bullying can impact negatively on a person's physical and mental health causing harm in the form of physical injuries, stress-related illness, depression and other health issues.
- Right to work and fair working conditions.[15] Bullying can lead to higher absenteeism from the workplace, poor or reduced performance and an unsafe working environment.
- The right to freedom of expression and to hold opinions without interference.[16] Bullying can impact on a person's freedom to express feelings or opinions as they no longer feel safe to do so.
- The right to be free from violence, whether physical or mental.[17]

Cyber Racism

There are many examples of cyber- racism on the internet from racist individual Facebook posts to group pages specifically set up a racist purpose.

Cyber-Sexism/Sexual Harassment

Instances of Cyber-Sexism are similarly numerous. Other examples of Cyber-Sexism, Sexual harassment include "Creep Shots" where man take pictures of intimate body parts of unsuspecting women snapped on the street or in their private places and load them on a publicly accessible website.[18]

Cyber Hemophobia

The incidence of homophobic cyber-bullying has increased greatly in recent years with the proliferation of online social networking tools.[19] In U.S.A, a student killed himself shortly after discovering that his roommate had secretly used a webcam to stream his sexual intimate actions with another man over the internet.

It is thus evident that the internet is being used in different ways to facilitate various forms of discrimination and harassment.

---

14 UDHR, Art. 25; ICESCR, Art. 12(1); CRC, Art. 24.
15 UDHR, Art. 23; ICESCR, Arts. 6 & 7.
16 UDHR, Art. 19; ICCPR, Art. 19.
17 UDHR, Art. 5; ICCPR, Art. 7; CRC, Art. 19.
18 http://www.dailylife.com.au/creepshots 27-08-2013.
19 L. Hillier, Horsley and C. Kurdas.

Intellectual Property Rights and Cyber Space

Intellectual property rights are the legal rights that cover the privileges given to individuals who are the owners and inventors of a work and have created something with their intellectual creativity.

Types of Intellectual Property Rights:

The following are the intellectual property rights:

- Copy Right
- Patent
- Trademark
- Trade Secrets etc.

The Government of India passed legislation in 1999 to safeguard the intellectual property rights.

- The Patents (Amendment) Act 1999 facilitates the establishment of the mail box system for filing patents. It offers exclusive marketing rights for a time period of Five years.
- The Trademark Bill 1999, replaced the Trade and Merchandise Marks Act 1958.
- The Sui generis legislation was approved and named as the Geographical Indications of Goods (Registration and Protection) Bill, 1999.
- The Industrial Designs Act replaced the Designs Act 1911.

Intellectual Property Rights and Cyber Space

As is well known any new invention in the field of technology has to face threats and the internet is no exception to it; which has captured the physical marketplace and have converted it into a virtual marketplace.

Immense need is felt to safeguard the business interest as a whole keeping in view the challenges, and to effectively manage the intellectual property, that the Cyber Space has also joined the main stream.

It is therefore evident, today it is highly regarded, considered to develop an effective and collaborative IP Management mechanism and protection strategy. Thus the constant threats in the Cybernetic World can be monitored and confined.

Various approaches and legislations have been designed by the law-makers to wake up the center in delivering a secure cyber threats. Despite this factor, it is the duty of the Intellectual Property Rights (I.P.R) owner to invalidate and reduce such malafide acts of criminals by proactive measures.

Cyber Space Use and Misuse

There is need to analyse the present status of use and misuse of internet by youth in India, especially the semi-urban and rural youth, where many girls became victims of cyber social networking sites (Halder & Chandrasekhar, 2009) and boys have become victims of the internet.

The reports of various agencies would tell how much the Indian youth has made internet communication medium such as "Google" and "Facebook", part and parcel of their every day affairs. It must also be noted that India has also shown sufficient growth towards e-governance and e-banking and this has been ensured by National Telecommunication Policy, 2012 (Telecom Regulating Authority of India (T.R.A.I) 2012). But at the same time, it also needs to understand that millions of internet users in India are unaware of cyber safety and security essentials (umarhathab, Rao & Jai Sankar 2009), netiquettes and proper forums for reporting crimes (Halder & Jai Sankar, 2010)

Internet and Digital Communication Technology (D.C.T) has created an enormous opportunity for people of all ages including student community to contribute and accumulate information. It is indeed not exaggerating that people are getting connected to each other through e-mails, chatting rooms, social media platforms like Facebook, Whats app, Twitter etc. The term "Social Network" is so popular that children and old (Senior Citizen) people are no exception in making use of this, which has now become a part of their daily life and without which they feel incapacitated. Internet and D.C.T also make it possible for users to avail online banking, shopping as well as e-library facilities. India also now boasts of almost higher rate of users of D.C.T and internet including popular social media (NDTV,2013) on par with western countries. This has been further motivated by government efforts through National Telecommunications Policy, 2012 which has maximised the reach of D.C.T and internet to people (T.R.A.I, 2012).

It is very interesting to note that the rural popular like their urban counterparts are now equally getting connected to D.C.T network and they are being encouraged to participate in e-governance

through various schemes. Schools, colleges and universities (inclusive of public and private funded) situated in the semi-rural, rural or interior parts are encouraging the use of I.T and D.C.T to their students. Because of the increase use of cyber space there has been stiff competition among the internet service providers to drastically reduce the charges for their usage, so much so not only the affluent families but lower income family groups are not hesitant to become, "netizens" a very popular "term" of the world today.

The findings of T.C.S (Tata Consultancy Services), Gen Y Survey 2012-13 of nearly 17,500 high school students (metros and tier-II cities) across 14 Indian Cities reveals that smart devices and unprecedented levels of online access are making this generation the most connected one and this is changing the way they communicate with each other and transforming both their academic and social lives (T.C.S, 2013).

There is a need to analyse the present status of use and misuse of internet by youth in India, especially, the semi-urban and rural youth, when many girls have become victims of cyber social networking sites (Halder & Jai Sankar, 2009) and boys become victims of abuse of internet.

Rothstein (2003) study showed that many preferred to stay online and avoid family gatherings and parties. The study further showed that women recognized behavioural problems and attempted to stop internet usage than men.

Parchar (2011) had shown the positive usage of the social media by the students as well as the higher educational institutions. The study had taken up the usage of popular social media like Facebook, Twitter, YouTube and the Indian websites like Bharatstudents.com etc. and shown that while students mostly use the platforms for connecting with seniors, classmates, faculty members and get information for opportunities abroad, many higher educational institutions apply social media marketing method to market themselves for prospective students.

The study also highlighted that even though various types of cyber-crimes are inevitable when using social media, growing member of Indian students are positively using the social media.

Alam, Yeow and Loo (2011), study particularly concentrates on online dating of the students. In this study, the researchers had found Facebook as the most popular online social networking site among Malayalam students. 79.63 %(highest) students indicated

that they use Facebook for sending and receiving messages and 67.20% indicated that they use it for communicating with their friends. The study further showed that majority of the students use social networking sites for passing time or to fight boredom. The researchers also showed that among the total respondents only 12.17% had gone for dating sites for seeking dating partners.

Ghorui (2012) has emphasized mainly upon the news consumption and dissemination by the students in the cyber space by using "uses and gratification theory". This theory was mainly used to find out the motives behind consumption and dissemination of the news in the cyberspace. The study showed that even though online consumption of news is lesser than offline consumption of the news, students use dissemination for relaxation and maintaining personal relationships.

According to Google (2013)[20] "Phishing is a form of fraud, in which a message sender attempts to trick the recipient into divulging important personal information like a password or bank account number, transferring money or installing malicious software. Usually the sender pretends to be a representative of legitimate organizations". This information is available in the G-MAIL services and it encourages users to mark mails as Phishing mails which bear such characteristics.

Halder and Jai Sankar (2010, Page No:12)[21] simplifies the definition of stalking by stating that "in one word, when "following" is added by Mens rea to commit a harm and it is successful digitally carried out, we can say cyber stalking has happened." It needs to be pointed here that the Criminal Law Amendment Act 2013 included the definition of the term stalking women in Sec.354 D (1) and it states: Any man who …. (i) follows woman and contacts, or attempts to foster personal interaction of disinterest by such women, or (ii) monitors the use by a woman of the internet, e-mail or any other form of electronic communication, commits the offence of stalking: provided that such conduct shall not amount to stalking if the man who pursued it proves that …. (i) it was pursued for the purpose of preventing or detecting crime and the man accused of stalking had been entrusted with the responsibility of prevention and detecting crime by the state; or (ii) it was pursued under any law or to comply with any condition or requirement imposed by any

---

20 *Google* 2013, 25-08-2013, http://support.google.com.

21 Halder & Jai Sankar, K. (2011) *Cyber Gender Harassment and Secondary Victimization: A Comparative Analysis of US/UK and India, Victims and Offenders*, 6(4), 386-389.

person under any law or (iii) in the particular circumstances such conduct was reasonable and justified.

Google (2013)[22] defines the term spoofing by stating "Spoofing means faking the return address on outgoing mail to hide the true origin of the message."

The Information Technology Act 2000 as amended in 2008[23] while prescribing the punishment for identity theft in S.66 C explains the term as fraudulently or dishonesty making use of the electronic signature, password or any other unique identification feature of any other person.

Cyber Laws (Information Technology Act, 2000 Amended in 2008)

So far, in the above paragraphs of this paper, detailed discussion has taken place with regard to Human Rights-Cyber Space use and misuse. With this backdrop, it will be pertinent to know about the consequences of the misuse of cyber space.

The faster worldwide connectivity has developed numerous online crimes and these increased offences led to the need of laws for protection. In order to keep in stride with the changing generation, the Indian Parliament passed the Information Technology Act 2000 (later amended in 2008) that has been conceptualised on the United Nations Commissions on International Trade Law (U.N.C.I.T.R.A.L) Model Law

The Law defines the offences in a detailed manner along with the penalties for each category of offence.

Cyber-crime usually includes the following:

- Unauthorized access of the computers
- Data didling
- Virus / worms attack
- Theft of computer system
- Hacking
- Denial of attacks
- Logic bombs
- Trojan attacks

---

22 Halder D & Jai Sankar, K. (2009), *Cyber Socializing and Victimization of Women. TEMIDA: Journal on Victimization Human Rights and Gender*, 12, 5-36 (Sept. 2009).

23 Manjunatha, S. (2013), *The Usage of Social Networking Sites among the College Students in IJSS*. http://www.csca.in/IJSS,25-08-2013.

- Internet time theft
- Web jacking
- E-mail bombing
- Salami attacks
- Physical damaging computer system

The offences included in the I.T. Act are as follows:

- Tampering with computer source documents
- Hacking with computer system
- Publishing of information which is obscene in electronic form
- Protected systems
- Penalty for misrepresentation
- Penalty for breach of confidentiality and privacy
- Penalty for publishing Digital signature certificate false in certain particulars
- Publication for fraudulent purpose
- Act to apply for offences or contravention committed outside India confiscation

The following table shows the offence and penalties against all the mentioned sections of the I.T. Act:

Section	**Offence**	**Punishment**	**Bailability & cognizability**
Sec. 65	Tampering with Computer Source Code	Imprisonment up to 3 years or fine up to Rs. 2 Lakhs	Offence is bailable, cognizable and triable by court of JMFC
Sec. 66	Computer Related Offences	Imprisonment up to 3 years or fine up to Rs.5 lakhs	Offence is bailable, cognizable and triable by court of JMFC
Sec.66-A	Sending offensive messages through communication service, etc.	Imprisonment up to 3 years and fine	Offence is bailable, cognizable and triable by court of JMFC

Sec.66B	Dishonesty receiving stolen computer resource or communication device	Imprisonment up to 3 years and / or fine up to Rs.1 lakh	Offence is bailable, cognizable and triable by court of JMFC
Sec.66C	Identity theft	Imprisonment of either description up to 3 years and/ or fine up to Rs.1 lakh	Offence is bailable, cognizable and triable by court of JMFC
Sec.66D	Cheating by personation by using computer resource	Imprisonment of either description up to 3 years and/or fine up to Rs.1 lakh	Offence is bailable, cognizable and triable by court of JMFC
Sec. 66E	Violation of Privacy	Imprisonment up to 3 years and / or fine up to Rs. 2 lakhs	Offence is bailable, cognizable and triable by court of JMFC
Sec. 66F	Cyber Terrorism	Imprisonment extend to imprisonment for life	Offence is non-bailable, cognizable and triable by court of sessions
Sec. 67	Publishing or transmitting obscene material in electronic form	On first conviction, imprisonment up to 3 years and/ or fine up to Rs.5 lakhs on subsequent conviction imprisonment up to 5 years and/ or fine up to Rs.10 lakhs	Offence is non-bailable, cognizable and triable by court of JMFC
Sec. 67A	Publishing or	On first	Offence is non-

	transmitting of material containing sexually exploit act, etc.… in electronic form	conviction imprisonment up to 5 years and / or fine up to Rs.10 lakhs, on subsequent conviction imprisonment up to 7 years and/ or fine up to Rs.10 lakhs	bailable, cognizable and triable by court of JMFC
Sec. 67B	Publishing or transmitting of material depicting children in sexually explicit act etc.… in electronic form	On first conviction imprisonment of either description up to 5 years and/ or fine up to Rs.10 lakhs on subsequent conviction imprisonment of either description up to 7 years and/ or fine up to Rs. 10 lakhs	Offence is non-bailable, cognizable and triable by court of JMFC
Sec. 67C	Intermediary intentionally or knowingly contravening the directions about preservation and retention of information	Imprisonment up to 3 years and fine	Offence is bailable, cognizable
Sec. 68	Failure to comply with the directions given by controller	Imprisonment up to 2 years and/ or fine up to Rs.1 lakh	Offence is bailable, non-cognizable
Sec. 69	Failure to assist	Imprisonment	Offence is non-

	agency referred to sub section (3) in regard interception or monitoring or decryption of any information through any computer resource	up to 7 years and fine	bailable, cognizable
Sec. 69A	Failure of the intermediary to comply with the direction issued for blocking for public access of any information through any computer resource	Imprisonment up to 7 years and fine	Offence is non-bailable, cognizable
Sec. 69B	Intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) in regard monitor and collect traffic data or information through any computer resource by cybersecurity	Imprisonment up to 3 years and fine	Offence is bailable, cognizable
Sec. 70	Any person who secures access or attempts to secure access to protected system in contravention of provision of Sec.70	Imprisonment of either decryption up to 10 years and fine	Offence is non-bailable, cognizable
Sec. 70B	Indian computer	Imprisonment	Offence is

	emergency response team to serve as national agency for incident response. Any service provider, intermediaries, data centers etc. who fails to prove the information called for or comply with the direction issued by ICERT	up to 1 year and/ or fine up to Rs.1 lakh	bailable, non-cognizable
Sec. 71	Misrepresentation to the controller to the certifying authority	Imprisonment up to 2 years and/ or fine up to Rs.1 lakh	Offence is bailable, non-cognizable
Sec. 72	Breach of confidentiality and privacy	Imprisonment up to 2 years and/ or fine up to Rs.1 lakh	Offence is bailable, non-cognizable
Sec. 72A	Disclosure of information in breach of lawful contract	Imprisonment up to 3 years and/ or fine up to Rs.5 lakhs	Offence is bailable, cognizable
Sec. 73	Publishing electronic signature certificate false in certain particulars	Imprisonment up to 2 years and/ or fine up to Rs.1 lakh	Offence is bailable, non-cognizable
Sec. 74	Publication for fraudulent purpose	Imprisonment up to 2 years and/ or fine up to Rs.1 lakh	Offence is bailable, non-cognizable

- Act to apply for offences or contravention committed outside India confiscation

The following table shows the offence and penalties against all the mentioned sections of the I.T. Act:

Action Plan-Task Ahead

The need of the hour is how to arrest/ check the misdeeds of the miscreants of cyber-crime which is now a challenging job ahead of the administration, departments and governments throughout the world, day in and day out. It is easily said rather than done. Indeed, it is a million-dollar question posed to the investigating officers, bureaucrats and the concerned authorities.

Despite law reforms, multifaceted actions by several fora there are no signs of decrease or reduction in cyber-crimes but the miscreants have chosen discrete actions in various forms and not being booked for obvious reasons.

It is now evident that upcoming years will experience more cyber-attacks. So organizations are advised to prevent their data supply chains with better inspection methods.

- Stringent regulatory rules are put in place by many countries to prevent unauthorized access to networks. Such acts are declared as penal offences.
- The growing awareness on privacy is another upcoming trend. Google's chief internet expert Vin Cerf has stated that privacy may actually be an anomaly.
- Cloud Computing is another trend. With more advancements in the technology, huge volumes of data will flow into the cloud which is not completely immune to cyber-crimes.

Developmental Areas

The "Cyber-Law trends in India 2013" and "Cyber Law developments in India in 2014" are two prominent and trustworthy cyber-law related research works provided by Perry 4 Law organisation (P4LO) for the years 2013 and 2014.

There are some grave cyber law related issues that deserve immediate consideration by the Government of India.

Following are some major issues:

- A better cyber law and effective cyber-crime prevention strategy
- Cyber-crimes investigation training requirements
- Formulation of dedicated encryption laws

- Legal adoption of cloud computing
- Formation and implementation of e-mail policy
- Legality of online gambling and online pharmacies
- Legality of Bitcoins
- Framework for blocking websites
- Regulation of mobile applications

With the formation of cyber law compulsions, the obligation of banks for cyber theft and cyber-crimes would considerably increase in the near future. Indian Banks would require keeping a dedicated team of cyber law experts or seeking help of external experts in this regard.

The transactions of cyber-insurance should be increased by the Indian Insurance sector as a consequence of the increasing cyber-attacks and cyber-crimes.

Expanding Cyber Security

Due to ever-increasing dependence on the internet, the biggest challenge we face today is the security of information from miscreants. Therefore, it is a must to promote research and development in cyber security, so that we can come up with robust solutions to mitigate cyber-attacks.

Cyber security research is the area that is concerned with preparing solutions to deal with cyber criminals.

Next Generation Firewalls

Multi-identity based expertise such as Next Generation Firewall that offers security intelligence to enterprises and enable them to apply best suited security controls at the network perimeter are also being worked on.

BYOD (Bring Your Own Device) and Mobile Security

Mobile security testing, cloud security and BYOD (Bring Your Own Device) risk mitigations are some of the areas where a lot of research is being done.

Cyber Forensics

Cyber forensics is the application of analysis techniques to collect and recover data from a system or a digital storage media or device.

Some of the specific areas where research is being done in India are:

- Disk forensics
- Network forensics
- Mobile device forensics
- Memory forensics
- Multimedia forensics
- Internet forensics

Role of Human Resource Department

H.R.D in every organization plays a pivotal role in arranging cyber security. H.R plays a key role in educating employees about the impact, their attitudes and behavior on the organization's security. The H.R team is best placed to advice whether policies are likely to work and whether they are appropriate.

It is possible that cyber criminals take the help of insiders in a company to hack their network. Therefore, it is essential to identify employees who may present a particular risk and have stringent H.R policies for them.

Cyber Security Awareness

It is high time that cyber security awareness is inculcated from the grass root level like schools where users can be made aware how internet works and what are its potential threats.

Every cyber café, home/personal computers and office computers should be protected through firewalls. Users should be instructed through their service providers or gateways not to breach unauthorized networks. The threat should be described in bold and the impacts should be highlighted.

The government must formulate strong laws to enforce cyber security and create sufficient awareness to public by broadcasting the same through television, radio/internet advertisements.

Sharing of Information

United States proposed a law called "Cyber Security Information Sharing Act 2014(C.I.S.A)" to improve cyber security in the country through enhanced sharing information about cyber security threats. Such laws are required in every country to share threat information among citizens.

Mandatory Reporting Mechanism

The recent malware named Uroburos/Snake is an example of growing cyber espionage and cyber-warfare, stealing of sensitive information is the new trend.

This problem can be addressed by formulating a good cyber security law that can establish a regulatory regime for obligatory cyber security breach notifications on the part of telecom companies/ISPs. Infrastructure such as automated power grids, thermal plants, satellites etc. are vulnerable to diverse forms of cyber-attacks and hence a breach notification programme would alert the agencies to work on them.

Conclusion

The elaborate discussion aforesaid on the subject boils down to arrive at the following conclusions to make an effective and worthy exercise in the matter of cyber space use and misuse linking with Human Rights.

1. Cooperation amongst authorities is often a matter of sovereignty and pride.
2. Reinforcement of the role of multinational companies presupposes the establishment of effective oversight mechanisms, also aimed at overcoming identified gaps.
3. Internet is one of the most powerful instruments of 21st century for increasing transparency in the conduct of the powerful access to information and for facilitating active citizen participation in building democratic societies.
4. The internet provides unparalleled opportunities for the promotion and advancement of Human Rights most certainly the right to seek receives and imparts information.
5. The internet also provides a new (and powerful) medium through which persons (and does) publish hateful or discriminating comments and intimidate and harass others, in a manner which undermines the Human Rights of those who are targeted.
6. The issues of consent, governance, privacy and surveillance and technology need to be coupled with analysis of ethical positions and legal positions and practices. Only in this way will there be a chance of protecting basic Human Rights and fostering responsibility in this digital age, failing which any amount of advancement is of no avail.