Chapter 8

Human right philosophy and control of Cyber-crime
Chapter 8
HUMAN RIGHT PHILOSOPHY AND
CONTROL OF CYBER-CRIME

8.1 Introduction

Cyberspace is the digital world created by virtual communicative space with the help of technologies. Today, Cyberspace is being used for everything from providing the suitable marriage partner to the making available private rooms for chatting. The Cyberspace displays on its counter everything that one can look for in real world. The activity in Cyberspace ranges from computerised reservation systems to automated teller systems. It is not merely the networking of computers but the platform of all social activities sharing maximum qualities of real world and real time.

The Cyberspace thus has markets, public and private chatting rooms, Cyber norms, hoardings, participating cyber-netizens, social and economical activities and displays analogous emotional spectrum. These analogies of people they emote in Cyberspace create different issues for the debate of social, political, economical, psychological which are also present in real world. The different level of these debates also includes the issues like 'Human Rights' in Cyberspace. Thus it is inevitable that human rights activists hurled upon to see the incidences of human rights violation in Cyberspace and raise their alarming voices against it. The part of this investigative writing will deal with to analyze issues by verifying the standard of human right philosophy in Cyberspace.

8.2 Governance in Cyberspace: Two approaches

While discussing the human rights issues in Cyberspace, and to start with the basic questions, the doubt may be raised that whether governance at all is possible in Cyberspace? Though Cyberspace by analogy shares the quality of real world, it does not have the same pattern of execution mechanism and governance level that appear in the real world. Again, in generally human rights [of distributive nature] are executed either against the State or by the State. Therefore interesting issues may attract the attention of ordinary observer like, -

Whether governance is possible in Cyberspace?
Whether governance in general and execution of Human rights are justifiable? And too what extent?

What would be the level of governance?

What would be the modality of execution of Human rights in Cyberspace?

To start with the first issue, it can be said that governance is possible in Cyberspace. Thought presently it appears that there is no Cyber police patrolling the web pages or chat rooms, but the international attempt of harmonizing the execution level will positively make Cyberspace more secure space and governing the Cyberspace is not far reaching dreams. Most of the State legislation already described the Cyber crime and declared certain act punishable. Therefore various nations within their national boundaries trying to govern the Cyberspace, (though Cyberspace does not respect national or geographical boundaries) it is possible to govern the Cyberspace.

The next issues are whether it is justifiable to govern the Cyberspace? There are some jurists labeled as anarchist or nihilist who agitate against the governance itself. For them, 'No governance is the best governance'. Rober Nozic for instance argue to have 'minimal state' where State should have limited power of interference with the liberty of an individual. There is the staunch anarchistic position that considers Cyberspace a totally new and alien territory where conventional rules do not apply. For those holding this Cyber-libertarian view (represented by visionaries like John Perry Barlow) no governance is the best governance.¹

8.2.1.1 No governance is the best governance: Nihilistic view

The basic contenders of this approach think that governance may cause interference in using the technology. It ultimately restricts the full fledged utilization of technology which is ultimately not justifiable on ethical or legal grounds. It by no means that Cyber world should be left unattained. It simply means that Cyber world will soon evolved its own norms where situation like 'one control all and all control one' will regulate the Cyber world. The minimal interference by Government is desirable.

Again the anarchists suggest that there is alternative to governance in Cyberspace. The inner response from Cyberspace by netizens is sufficient for controlling mechanism in Cyberspace. The Cyberspace can best police by itself and a variety of forms of self regulation ranging from Parent Control software to Cyber Angels, Codes of Conduct and Netiquette.

8.2.1.2 Governance is ultimately promote the utilization: Utilitarian's view

However, another approach can be adopted where it can be contended that by governance, the utilization will promote. Here interference or governance will enhance the security aspect and thus Cyberspace will be the safer place than ever. For maximum utilization, the net population should feel free and protected against its misuse. Governance by no mean disturbance and legal norms control human behavior in the Cyberspace will by no means threats to the law abiding netizens. The opponent of the nihilist and Cyber-anarchist would want a strict regime for activities in Cyberspace to control the pornographers, copyright pirates, hackers or just anybody who holds politically subversive aspirations.

8.2.2 Cyberspace should be governed to protect and promote Human Rights

Though, whatever may be the approaches adopted by these legal thinkers, and whatever attractive these approaches may seems to be, if increasing number of people are habituating in Cyberspace it need to be regulated by scientific policymaking. This is equally true because if Cyberspace is to be protected against unprecedented opportunities for criminal activity, systematic infrastructure based on planed policymaking has no alternative. The argument can also be supported because though Cyberspace technology has created virtual world, it by no means differ and de-linked from the norms of real world. In fact, the citizens entered into Cyberspace as netizens with all their experience, language, feelings, human sensitivity to make Cyberspace alive, else it is nothing but the moving electrons.

8.3 Human Right philosophy in Cyberspace

8.3.1 Brief history of emergence of Human Right philosophy at International scene

Basically the concept of 'Human Right' can be traced as back as the origin of human civilization. And from time immemorial we can find some imprint of agitation
for restoration of human right against the agencies of human right violators. 'Magna
Charta' and 'Bill or Rights' are some of the incidences in human history where peaceful
way was adopted by citizens for guaranteeing the human rights to their respective
political authority. However, these incidences are restricted to politico-geographical
boundaries and equally, and significantly, but not having more impact beyond specific
territorial boundaries.

The 'Human Right' has shaped only after Second World War when world
witnessed the assaults against human dignity during war and ultimately the United
Nation began to develop a universal framework of moral standards. This was to become
the international human rights regime.

This novel ideal of the international human rights regime, as it was established
after 1945, was the articulation of the age old struggle for the recognition of human
dignity into a catalog of legal rights. Now the world community has shifted its attention
from "rights of man" to the more comprehensive "human rights".

Previously, the 'human rights' whatever may be in the forms and features, was
the national affair, but when UN had declared it as one of the subject on its agenda, was
put on the agenda of the world community. Herewith, the defense of fundamental rights
was no longer the exclusive preoccupation of national politics and became an essential
part of world politics. The judgement whether human rights had been violated was no
longer the exclusive monopoly of national governments.²

This international incidence extends the availability of Human Rights to a
common man which is now no longer restricted to privileged individuals and social
elites class. Now Human Right is the regime where approach is "all people matter".
These basic rights of human being were to be inherited rather than conferred and apply
to everyone and to exclude no one.

The regime of human right was evolved while the passage of time since 1945
and breathe through the conventions and commission. It evolutionized around the text
either in the way of international treaties, conventions, commissions or nation
legislations, some time binding in nature sometime of customary ways. The milestone

² Hamelink Cees, 'Human Rights in Cyberspace', Published at http://www.religion-
online.org/showarticle.asp Accessed on 15.11.2005 at 14.16.25
in this path was United Nations Universal Declaration of Human Rights\(^3\) and the two key human rights treaties, the International Covenant on Economic, Social and Cultural Rights\(^4\) and the International Covenant on Civil and Political Rights.

In these three documents (commonly referred to as the International Bill of Rights) one finds seventy six different human rights. If one were to take totality of some fifty major international and regional human rights instruments, the number of rights would obviously increase even further. There is also presently a tendency among human rights lobbies to put more and more social problems in a human rights framework and thus to add to the number of human rights.\(^5\)

### 8.3.2 Human Right philosophy in Cyberspace - How so far relevant?

It is interesting to discuss the relevancy of Human Right philosophy in Cyberspace. This is now beyond criticism that Cyberspace also shares the emotions and values. Conceptually and conventionally, the word 'Human Right' can be understood with existence and fulfillment of some basic requirement essential for giving shape to 'human' qualities to the physical existence of human being. These requirements include some of the basic needs to be supplied and equipped with. The concept of 'Human Right' can also be understood in terms of its correlation with level of implementation and standards of agencies that provide ample scope of protecting human sentiment in civilization.

Conventionally, Human rights are used to understand with restricted sense. It was characterized by exaggerated emphasis on the right-oriented model where conferring right and making remedies available in case of their violations are basic index of judging the standard of human right in society. The interpretations of Human Right limited around the concepts like 'freedom', 'equality', 'liberty', 'existence', 'survival', and 'remedy'. However, these conventional concepts completely ignore the issues that are more crucial in judging the reshaping of 'Human Right' in post-modern period. Those are, 'institutional base', 'Historical perspective', 'human weakness', 'fact skepticism', or 'rule skepticism' or 'realism'.

\(^3\) See, UDHR adopted on December 10, 1948 by the UN General Assembly
\(^4\) In force since January 3, 1976
The problem of regulation of human rights markets is not just state-centric. The investor, as well as the consumer, and communities, are stakeholders. The investor-based regulation takes myriad forms of channeling and controlling human rights agenda and transactions, generating a product mix that is the very essence of an audit culture (of upward accountability and line management). However, the investors themselves may be regulated, in response to which they must manufacture legitimation with the host society and government in ways wholly propitious with cross-border markets in human rights protection and promotion.\(^6\)

Thus presently in post-modern period, there are several issue are involve in shaping the 'Human Right' philosophy.

### 8.3.3 Applicability of Human Right philosophy in Cyberspace

In Cyberspace most of the activities are resembled with the activities of real life. It also involves all the emotional and value patter that appear in daily life of the person. Therefore, in order to understand Human Rights in Cyberspace, one should not have to adopt individualist approach. In Cyberspace, both individual and collective rights exist.

To put it in another way, it is observed that today Cyberspace is accessible to few elites who are in position to enjoy technology. There is ongoing debate about the unevenness of access to the means of communicating using digital technologies and about whether, and the extent to which, measures should be taken to reduce the effects of various types of digital divides.\(^7\) Today percentage of juvenile and women netizens are very less and poor are almost zero. Today, Information technology is branded as mechanism of upper class.

Thus Human right philosophy demands to have accessibility to Cyberspace to all those who are needed and can be benefited by its irrespective of their class.

---


and creed. Today, computer networking has spread horizontally to the advantageous strata, but its availability does not percolate vertically. The 11% population of world using computer includes those who are of developed and developing nations having rich resources to their credit. However, today, computer technology has potentiality to change thousands of life. Speaking with example the disabled person either unable to speak, hear, or read can use this technology. Special software can be developed to equip them to overcome their physical difficulties. Thus the people who are blind can use computer technology to read the newspaper as such types of speaking software are available in the market. Today, computer technology helps them by provided audio-visual aids.

Thus accessibility of compute technology should be ensure too all. 'All that matter' should be the basic motivational factor in this regime. The women, juvenile, the person of merit standards but poor must have facility to use it. Unfortunately today, computer networking has economic driven force behind it. The money is matter here. Thus is clearly violation of human rights of the society. Just like language, technology is also social property and no class or group can patent it for its personal use.

The same argument can be stretched in the area of education. Computer and information technology can be utilized in educational sector to its greatest extend. The information, knowledge, books, journals, digital libraries, articles can be made available to budding students who will be the assets of the society. Therefore, 'Right to access' should be recognized into the Cyberspace and its accessibility should be vertically extended where 'all matter and nobody should left'.

Thus Computer and Information Technology can be considered as 'information capital' and everybody should have right to inform. Right to inform here implies the capacity to process and apply information resources, the technical skills to manipulate ICT and the financial means to secure access to and use of digital networks. In national and global social realities the distribution of information capital is highly skewed.
This is reinforced by growing income inequalities across the world\(^8\) and the concurrent lowering of educational standards, and decline in status and salaries of teaching staff, and shifts in educational programmes from critical reflection to training for economic productivity and the dramatic loss of credibility political institutions face almost everywhere. The "freedom to" implies the entitlement to those socio-economic conditions that support the development of "information-capital".\(^9\)

The basic argument here is that everybody should be free to use the Cyberspace where he/she can visit information superhighway. Thus right to be informed is the key motivational factor here. However, though all fundamental technology is social capital and equal entitlement principles should be applied, may be with commercial reservations. Today the Cyberspace resources which is one of the basic nourishment for human brain and personality is highly threatened by the current economical order. Today, 'pay and use' system is applicable where the person having financial capacity to buy Internet hours can access it, however, the poor who cannot pay it, excluded from its use. During the course of time, it creates gap and 'knowledge' is being 'patent-ised' for class having accessible capabilities. Due to the same fear in mind, Karl Marx always propounded for common ownership of social capital to ensure its use by everybody. Speaking with statistics, only 5% of the citizens of developing nation has telephone lines and this ratio is even less in underdeveloped countries. Again in India 0.11% of the population is Internet user. Today, government or other organization either at national or international level do not seriously analyze these facts. In India, today an average charges for an Internet hour from Cyber café cost around Rs. 25/- which is almost two third of daily income of 40% population who are marginally around poverty line. Ironically, agricultural labourer who are 70% of all kind of labourers use to earn Rs. 40/- per day when his demand is very high. Thus higher cost of technology is nothing but the denial of technology. Generally whenever we talk about the spreading speed of technology in modern days, we are concerned with this elite's class only who are capable for using technology.

---

\(^8\) by what could be termed the "globalization of poverty"

The above discussion is not only true about an individual but it is also true about the nation. Today, there is complete imbalance of information & technology. The developed nation are having technology with them which is utilized by them to exploit the poor nation. Books, publications, e-journals, popular websites are belongs to rich nations and poor nations are just reduced as consumer for the present technology. This is again a major issue where information has been commoditized by western countries.

A form of governance for Cyberspace that takes equal entitlement to its resources seriously requires far reaching changes of the current political practices in such areas as development assistance, transfer of technology, intellectual property protection, and space cooperation. These practices all reinforce the inegalitarian character of the present global order. Changes would include a drastic increase in overseas development assistance in the field of communication and under conditions more favourable to recipient parties, the adoption of the UNCTAD Code of Transfer of Technology on the terms proposed by the developing countries, a revision of provisions on the protection of intellectual property in the GATT/TWO multilateral trade accord so as to take the interests of less powerful countries and small producers into account, and the adoption of a multilateral accord on space cooperation and equal benefits.\(^\text{10}\)

Today, human rights advocate raise their voices against the torture, custodial murder, sexual harassment but not against poverty. The information technology today is causing complete imbalance of in technological resources. The western countries are having market of software’s, antivirus, and other important commodities in Cyberspace. They are in the position of shopkeeper. As they are ready and capable to invest the initial amount, they can employ the software engineers to develop it. Generally these software’s engineers are basically from the poor nation. This causes much hard to poor nation basically in two ways. First they loss their brain talent due to ‘brain drain’ or migration of these intellectuals to the western countries and at the same time, they have to purchase the high cost technology from the western country which is prepared by their own non-residence software engineers. This is equally true about India.

\(^\text{10}\) Hamelink Cees, 'Human Rights in Cyberspace'; Published at http://www.religion-online.org/showarticle.asp Accessed on 15.11.2005 at 14.16.25
Today, all are aware about the technological asset we are having. The best of the world's software's and hardware's engineers are from India. Even though we are backward, because our nation is facing the problem of 'brain drain' in IT sector. The best engineers just fly abroad when they are in fact in position to serve the nation. While they serve the foreign nationals we are purchasing the technology in which they had invested their talent.

It is demand of human right philosophy that such exploitation should be stopped. There is difference between life and business. Even the IMF and other banks also impose certain condition on the poor nation. It is highly recommended that Cyberspace should be democratizing and the planned policymaking should be initiated to move it on the line of 'Welfare Cyberspace'.

Today, the Cyberspace is just like plastic world where human civilization behaves like machine. Man is losing its living character and become adroit. The Cyberspace though resembles with real world, it is losing its socialization. Thus in Cyberspace, the human behavior is just like machine and hardly there are any social norms which control human behavior in Cyberspace. The Human right under such circumstances is merely at stake.

Another problem in Cyberspace, which is the most concern today and related with Cyber crime is the security aspect. Today Cyberspace become very danger zone where the reputation, intellectual property, data, information, money is completely at risk. Everybody is having some mark and identity crises create maximum threats to those dealing in Cyberspace. Under such circumstances, there are frequent incidences of abuse, theft, attacks.

Human security is to-day jeopardized by fundamental risks induced by the process of modernization and its global spread. There are risks related to economic mal-distribution -the growing income disparities in the world and the globalisation of poverty entail lethal risks for increasingly large numbers of people in the world. There are risks related to ecological catastrophes (the desertification, the depletion of the Ozone layer, the deforestation, the Greenhouse effect). There are industrial risks such as a multiplication of the Bhopal catastrophe. There are risks related to the proliferation of nuclear arms and
conventional arms (e.g., biological and chemical warfare). There are risks related to bio-technological experimentation and genetic engineering.

There are also social risks related to Cyberspace-technology. These include nuclear warfare triggered off by computer malfunctioning, large-scale financial frauds, technological addiction, and aviation disasters. Intentional harm is easily inflicted in Cyberspace. Computer networks enable people to communicate in anonymity. Anonymity brings out the worst in people. Under the cloak of anonymity people engage in harmful acts against others through abuse and deceit. Apparently, anonymity creates a 'moral distance' to the victim, which makes it easier to commit harmful acts. It is the classical case of the bomber pilot who pushes the button and never knows who was hit. The Information Superhighway creates enormously attractive opportunities for 'digital crooks' and 'Cyber-snoopers'. Such crimes and misdemeanors that range from copyright infringements to electronic surveillance pose serious threats to people's moral and physical integrity.

Cyberspace-related social risks to human security are also induced by the increasing dependence upon vulnerable and error-prone digital systems. A risk factor is also the Cybernisation of daily life that reinforces current trends towards high-speed, robot-centric societies.¹¹

8.3.4 Technological impulses should not override the Human right philosophy

The new technologies have placed a powerful new tool in the hands of the international human rights movement. But that technology is only as good as its users are visionary. The Internet can create millions of followers but only if those who love freedoms are willing to lead.¹²

8.4 Human Rights in Cyberspace: The response of United Nation

In December 2003, the World Summit on the Information Society (WSIS) was convened under the auspices of the United Nations. This meeting aimed to stimulate

¹¹ Hameink Coes, Human Rights in Cyberspace, Published at http://www.religion-
online.org/showarticle.asp Accessed on 15.11.2005 at 14.16.25

action to ensure that the information societies emerging today are more, rather than
less, equitable than the societies that have preceded them. Human rights in the digital
age are openly being contested today. The text of the WSIS Declaration of Principles
espouses a common vision of the information society, particularly with respect to
human rights. For example:

'We reaffirm the universality, indivisibility, interdependence and
interrelation of all human rights and fundamental freedoms, including the right
to development, as enshrined in the Vienna Declaration. We also reaffirm that
democracy, sustainable development, and respect for human rights and
fundamental freedoms as well as good governance at all levels are
interdependent and mutually reinforcing. We further resolve to strengthen
respect for the rule of law in international as in national affairs.

'We reaffirm, as an essential foundation of the Information Society,
and as outlined in Article 19 of the Universal Declaration of Human Rights,
that everyone has the right to freedom of opinion and expression; that this
right includes freedom to hold opinions without interference and to seek,
receive and impart information and ideas through any media and regardless
of frontiers. Communication is a fundamental social process, a basic human
need and the foundation of all social organisations. It is central to the
information society. Everyone, everywhere should have the opportunity to
participate and no one should be excluded from the benefits what the
Information Society offers.

Nothing in this Declaration shall be construed as impairing,
contradicting, restricting or derogating from the provisions of the Charter of
the United Nations and the Universal Declaration of Human Rights, any
other international instrument or national laws adopted in furtherance of
these instruments.'

The Declaration goes on to emphasise the need to foster an inclusive
information society and to ensure the ability, not just to access information and to

12 World Summit on the Information Society (2003) 'Declaration of Principles', WSIS-
03/GENEVA/DOC/4-E, 12 December. Quoted from, http://www.itu.int/dms_pub/itu-
at 16.05.22
communicate, but also to contribute. Observations are made about the need for capacity 
building and for an enabling institutional and legal environment. On issues of building 
confidence and security in the use of information and communication technologies 
(ICTs), the Declaration has this to say:

'Strengthening the trust framework, including information and network 
security, authentication, privacy and consumer protection, is a prerequisite for 
the development of the Information Society. ...'

It is necessary to prevent the use of information resources and 
technologies for criminal and terrorist purposes, while respecting human 
rights....

All actors in the information society should take appropriate actions and 
preventative measures, as determined by law, against abusive uses of ICTs, such 
as illegal and other acts motivated by racism, racial discrimination, xenophobia, 
and related intolerance, hatred, violence, all forms of child abuse, including 
paedophilia and child pornography, and trafficking in, and exploitation of, 
human beings'. 14

Issues of trust, protection from criminal behaviour, and the applicability of 
international and national legal frameworks are clearly signposted in the WSIS 
Declaration. The declaration is accompanied by a Plan of Action.15 The actions 
envisaged are numerous and are aimed at reducing 'digital divides of many different 
kinds'. However, the documents are silent with respect to how existing and new 
interpretations of the law should apply nationally or internationally and on whether 
variations between countries mean that the Internet makes law enforcement virtually 
impossible.

Following the WSIS there has been much discussion about whether the Summit 
simply provided a costly opportunity to foster a hollow rhetoric about the need for 
'digital solidarity' or whether it succeeded in mobilizing a major step-shift in the 
priority that will now be given to finding the resources to implement the high ambitions

14 infra 10, paras. 35, 36. of WSIS Report
December. Quoted from http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-
0005/1MSW-E.doc Accessed on 12.02.2006 at 14:16:39
of the authors of the Declaration and Plan of Action. A clear call is made for research to unveil the causes and consequences of developments in all of the facets of the digital age.

8.5 Human Right in Cyberspace: General Observations

An essential prerequisite if the respect for human rights embedded in various national and international levels strived for, the real spirit of conceptual propagation should upheld. It is necessary to make surveillance about the execution of these principles, investigation of the way legal institutions, practices and interpretations are influencing today’s information societies. An important aspect of this field of inquiry is research on the way Cyberspace is being experienced by people in the very disparate contexts of their everyday lives. These issues require to be kept alive from a variety of vantage points. The main focus point of this surveillance of human action and human rights in those instances where it is mediated by the technologies of the digital age and encompasses a wide range of issues including the production and consumption of digital content, the means of control over unwanted intrusions to individual’s privacy, and emerging means of governing in Cyberspace. It is crystal clear now that, either globally or locally, today’s information societies are underpinned by digital technologies. These technologies enable applications that may be empowering for some people, allowing them to develop new ways of seeing the world around them. Ubiquitous networks are at the heart of the digital age. They are becoming familiar to people in all parts of the world, albeit, unevenly so. The Internet allows for use of Chatrooms, email, and voice communication by people representing numerous interests, values, and aspirations. Together with the World Wide Web’s enormous repository of information, the Internet is limited in its application only by the limits of human imagination. Within the digital spaces – or Cyberspaces – of this century, there are many opportunities for new forms of business and governance as well as for new forms of criminal or unwanted behaviour. Many of these also create the potential for changes in behaviour and perceptions of the non-virtual world. One of the key findings of recent research on the way digital technologies and the Internet are mediating our lives is that off-line conventions and practices do not diminish in importance in the face of new Cyberspace developments. In some cases, Cyberspace simply offers a complimentary space to conduct familiar activities, while in others, the new virtual spaces amplify existing activities or create opportunities for completely new activities.
and behaviours. While many efforts are underway to foster e-strategies for the development of new forms of electronic commerce and electronic government as well as host of other applications, the darker side of Cyberspace is often shrouded in mystery or revealed only by the media as ‘moral panics’ over signs that the Internet is untrustworthiness or that the riskiness of Cyberspace is substantial. Such type of efforts definitely offers a research-based assessment of the implications of the law and its evolving institutions for the protection of human rights and greater equity in Cyberspace developments.

8.6 Human Rights in Cyberspace: Issues, challenges and prospective

In order to analyse the human right in digital era, the Cyber-sex phenomenon is one of the area where the sexual exploitation of women use to takes place. The digital technologies helps in one or the other way to provide a means of communication making prostitutes easily available, or pornographic material easily accessible. The World Wide Webs are also one of the cheap sources for information exchange or material dissemination. Engaging women in sex trade is now global phenomena which enable women to see new opportunities on better terms, but ultimately lead to their exploitations. However, greater demand of pornographic material and their easy dealing via digital world also put women for commoditization of their dignified repute. Sometimes, even the incidences are there where Cyber-stalker uploads the nude photographs of girl on pornographic site for putting them under harassment. These sites easily make this technology available to upload such material without any scrutiny. However, the technology today, is harmful in too many respects to the women. Cyber-stalking, ‘virtual’ is pimping out and an intensification of harm and exploitation. Though, human rights are being recognized and legal and socio-economic

---


18 The incident took place on Dec, 16, 2005, around midnight at the CEDIT centre within the University Campus of Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, when two guys upload nude photographs of their classmate on the Websites of famous sexygirl.yahoo.com alongwith her address and phone numbers which latter on come to the notice of girl when she had started to receive calls. Interesting point to note here is that, the Yahoo makes such thing easily possible for any viewer to upload any photographs, without being scrutiny which is capable to spoil the life of any innocent person. In the present case, website refuse to accept any responsibility for any indecent material uploaded by anybody. See for more details, http://www.Cyberlawyer.in/wp/?p=12. Accessed on 23.02.2006 at 23.11.26
solutions to protect women from sexual exploitation are being devised, it is hardly, seems practical utilization of this bookish philosophy into ground reality in Cyberspace. It's seems a wide gap between what we preach and what we practice. There is little recognition that civil and political rights are 'gendered'. The Cyber-sex trade no longer necessarily involves movement and travel, creating new challenges for legislators and it continues to be unclear as to the circumstances under which consent may be deemed to have been given or not given in Cyberspace.

There is another area of human right violation in Cyberspace. The Juvenile protection against vulnerability is the core area for the human rights. The infringement of children's rights is either by way of child pornography, or even commoditization of Cyberspace making them virtual sickness, throwing them into digital world ignoring parental responsibility are some of key area in this regards. Digital technologies not only make it easier and less costly to produce pornographic content, but software can also be used to produce 'morphed' images which fall uncertainly within the ambit of existing law. Anonymity and closed Internet-based membership communities also protect paedophiles, make content production a potentially lucrative activity, and enable contacts to be made with children on- and offline. Although there is a Council of Europe Convention on Cyber crime which deals with child pornography, however, there are certain lacunas and loopholes which make the trade and practices possible in Cyberspace. The existing legislation such that the meaning of 'possession' of child pornography is 'open' to question because of the immaterial nature of this form of digital content.

8.7 Governance, Liability and Balance

Hate speeches are also to some extent responsible for violation of human right in Cyberspace, but most of time fall outside the legal jurisdictions due to trans-national nature. It is observed that implications of Cyberspace for the control of hate speech, begins with the 'no society in the world has concluded that free speech is an absolute barrier to state regulation of harmful expression'. The governance of Cyberspace is often said to be beyond the capabilities of the nation-state. It shows how differences in national law have implications that make it very difficult to achieve a universally applicable definition of how to protect human rights in the face of the propagation of hate speeches over the Internet. The prevailing view is that the best way to counter hate
speech is rebuttal by others, rather than by sanctions imposed by the state. It is also the cases that hate speech laws may be enforced against marginalized members of society, succeeding only in amplifying resentments. Neither hate speech laws nor a laissez faire approach address the underlying problems of poverty, social isolation and ignorance that give rise to group hatred. The difficulties of governing the Internet are posed as matters for social policy as well as for legislators. Closely related to this issue is the appropriate balance between the protection of reputation from defamatory speech and the right to freedom of expression.

Defamation can be defined as statements that are ‘injurious to the reputation or dignity of the person alleged to be defamed, it must be published or communicated to another who must understand its connection with the person allegedly defamed’. ‘Defamation is lower down the image in the estimate of others’.19 It can be shown, in practice, that there is a ‘hierarchy of speech’ protection. Internet-mediated speech raises issues including the standard to be applied, where publication is deemed to occur and the jurisdiction within action can be taken. Should liability fall only on the originator of an allegedly defamatory statement or on an Internet Service Provider (ISPs)?20 The attention can be drawn towards the potentially ‘chilling’ effects of imposing liability on the latter, such that ISPs may remove information even before there is judicial verification that it is defamatory. Despite the potential of the Internet to amplify defamatory speech, it can be insisted that ‘the application of existing legal rules and pre-existing tension between rights of reputation and those of free speech’ should pertain, notwithstanding the fact that the stability of the law and its enforcement are challenged by the global reach of the Internet and many different local legal and cultural norms.

---

19 See Section 499 of Indian Penal Code, 1860.
20 Please see, S. 79 of the Information Technology Act, 2000. In India Network Service Providers are conferred ‘Presumption of innocence’.

79. **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 thereunder 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;
If we stress this issue of ISPs liability further, we can be led to an argument that ISP should be primarily held responsible for the context of liability for failure to remove potentially harmful content, or failure to offer the required consumer protection. The present legislation in India is silent to this regard and ISPs are set free from most of liability with presumption of innocence in their favour. Existing legislation envisages ‘a form of notice and take-down procedure’, but it remains unclear what constitutes ‘knowledge’ and what time frame is applicable for judgements about an ISPs liability or immunity.

Guarded under these rights, it is interesting to argue whether ISPs will take it upon themselves to function as the moral guardians of Cyberspace. Again there are issues of balancing rights and obligations. If over-zealous ISPs refuse to host certain types of internet sites, they may jeopardize free speech rights. Alternatively, ambiguity about ISP liability could mean that ISPs permit the provision of content without regard to its potentially harmful effects.

8.8 Digital Divides in Cyberspace

There is ongoing debate about the unevenness of access to the means of communicating using digital technologies and about whether, and the extent to which, measures should be taken to reduce the effects of various types of digital divides. After all, there are many other major claims on the scarce resources of time and finance to support health care, education, economic development, or democratic governance. Another question about an empirically grounded account of why a binary distinction between those with and those without access to the Internet is unhelpful in thinking about what steps should be taken by legislators to address the numerous and differentiated uses of the Internet. It has been examined that Internet use to support commercial activity. However, for the protection of small and medium sized enterprises in developing countries, particularly, it needs to effort to introduce uniformity in the law governing electronic transactions often embody a ‘techno-centric’

---

logic which runs counter to people's experiences and preferences for how and with whom they choose to trade. As can be demonstrated, user and use-centred approaches to analyzing behaviour associated with the spread of the Internet, have a much greater potential to shed light on the complex and multi-faceted issues that legislators and legal experts face in the digital age.

8.9 The Technologies of Governing

The foregoing discussion is concerned mainly with choices and actions on the part of human beings who interact with digital technologies. However, the spread of the Internet is encouraging the development of technologies that can be used by individuals, or programmed as software agents, to filter, block and rate content that is available to end-users. While the market for these technologies has not grown nearly as rapidly as initially expected and there is little harmonisation or interoperability of approaches, these technologies raise crucial issues about the nature of the 'public sphere' and about censorship.22

The interesting question can be raised, 'Whether free speech has any value if it cannot be heard?' It is experienced with filtering technologies and content rating initiatives that if the 'gatekeeper' approaches is adopted for the access to such vulnerable material, the present generational can be protected too some extend from such instances. This aimed at limiting access to illegal, harmful and racist content on the Internet. New technologies can be institutionally mandated for use, for example, in libraries to prevent children's access.

The another more important and crucial question is 'will the Internet remain a true “marketplace of ideas”, a blowsy bazaar of the bizarre to the banal, or will filtering technology transform the experience of many users into something akin to a Communist-era department store, where choice is limited by central governance?' These technologies also make it feasible for end-users' prejudices to become embedded in the technology, making their use and effects anything but transparent over time.

Another stance can be taken up about the theme of state intervention as a form of Internet governance. In this case the discussion of filtering, self-censorship and the

practices of states focuses on efforts to limit access to content for political reasons.\textsuperscript{23} Quite apart from the fact that filtering can lead to errors and mistaken or unintended blockages, the notion that the Internet is inherently open because of the nature of its architecture is not one that can be sustained in the light of current technological developments and various methods of fostering self-censorship. The experience of China where citizens are encouraged to make ‘public pledges’ not to publish information of certain kinds. Elsewhere, Internet Café owners are often required to block certain kinds of content. In the US legislation requires libraries and schools to block content to protect children.\textsuperscript{24} The specter of the ‘strangulation’ of the open Internet and point to various ways in which Internet filtering software is being used in ways that elude public scrutiny of the types of content and Web sites that are excluded. The new technologies of governance do not always support the empowerment of civil society movements.\textsuperscript{25}

The variety of means by which virtual community actors use the Internet can be controlled with respect to their use of content that is subject to intellectual property protection. In the case of Napster and subsequent efforts by the music industry to prosecute individuals who download music which is subject to copyright protection. Current copyright protection of digital content and software provides a completely inappropriate ‘blanket, one-size-fits-all solution’.

When software is so protected, creative efforts to develop new applications are suppressed since any effort to reuse or build upon the software code becomes an infringement of the law. It can be suggested that the practice of registration of

\textsuperscript{23} The broader issues in this area are discussed in Kalathil, S, and Beas, T, Open Networks: Closed Regimes 2001, Washington DC: Carnegie Endowment for International Peace.

\textsuperscript{24} Though it appear that similar suggestions were levelled by the Commissioner of Police(CP), Delhi white discussion of 79\textsuperscript{th} Report on the Information Technology Bill, 1999, on 4\textsuperscript{th} May, 2000 to the Committee. See, for e.g.

The Committee in its meeting held on 4\textsuperscript{th} May, 2000 had the benefit of the presentation made by the Commissioner of Police(CP), Delhi. The CP stated, \textit{inter alia}, that in order to prevent Cyber crimes, all Internet Service Providers should allow internet access through the digital telephone only which would enable to keep records of caller identification in the respective server. He also expressed concern on the mushrooming of Cyber Cafes from where a criminal mind could easily cause damage in economic terms. In order to provide solution, he suggested insertion of a provision regarding identification of particulars of the user through ration card, electoral card, passport, driving license, PAN Card etc. An obligation should be imposed on the ISP to maintain a record the users and provide details of every Cyber activity.\textsuperscript{19} However, the proposal was discarded by putting an argument that this will closed down all the Cyber cafés in India, which will again create problems with right to accessibility. For more details please see, \url{http://rii frayabha.nic.in/book2/reports/science/79report.html}

copyrights before they take effect offers a means of providing appropriate and differentiated levels of protection.26

One of the reasons that states seek legal means of intervening in Cyberspace is to counter Denial of Service (DoS) attacks on Internet servers. It can be differentiated between civil disobedience, criminal activity and terrorism. Each of these has different legal implications. The meaning of the term terrorism is changing such that emphasis is being given to whether fear is engendered rather than to the extent of violence or devastation. Whether they are the result of coordinated action or the actions of a single individual, DoS attacks can completely overwhelm Internet servers.

In consequence, legislative measures are being put in place. These include the European Union’s Cybercrime Convention, European Council Framework Decision on Attacks against Information Systems and the UK Terrorism Act. These measures aim to reduce the likelihood of such attacks. When such attacks represent a form of civil disobedience and democratic protest, they should not be criminalized. The right to free expression should not be limited without evidence of a clear threat to society. However, it can be argued that current measures are likely to jeopardise human rights.

8.10 Privacy and Surveillance

Cyberspace raises many issues for privacy protection. Privacy focusing particularly on control-based definitions emphasizing the individual’s autonomy to determine what is kept in the private sphere in contrast to those who regard the social importance of transparency as a collective value that should be considered. The issue of whether privacy should be regarded as a unique or a derivative right is debatable.

Under the backdrop of Right to Information Act, 2005,27 most of the laws, relating to official secrecy,28 data protection legislation29, and laws on confidentiality, highlights the ambiguity of the law. For instance, it is unclear whether the Human

27 See, Section 4 of Right to Information Act, 2005 passed by Central Government bring into operation on 12.10.2005.
29 See new suggested amendment by Expert Committee about data protection in the IT Act, 2000, specifically see Chapter 6.3.2 (9) of this investigative writing.
Rights Act 1993\textsuperscript{30} in India created a right to the protection of privacy via an extension of the law of confidentiality. There are unanswered questions about how privacy infringement should be valued and about the meaning of informed consent with respect to the use of information on the Web. The digital age has spawned many new techniques of surveillance and these have been applied increasingly extensively within the workplace.\textsuperscript{31}

It can be further stressed how the law attempts to reconcile employee’s perceptions of the right to privacy with employers’ interpretations of employment relationships. Common law does not provide employees with a general right to privacy in the workplace, but most of the human right laws may have conferred new rights. Though by ‘Vishakha’s’ case, some rights against sexual exploitation has been ensured to women. But, whether, under the new setup of economic order such as outsourcing industry, where several jurisdictions are involved, what and how so far the rules of national legal system are efficient and effective?

However, the new legislation on curtailing employee surveillance (monitoring telephone calls and email communications) is likely to be slow to take effect. On balance, merely the Art. 21, of the Constitution is neither coherent nor straightforward in protecting employees’ privacy in the workplace. In the absence of clarity about how much privacy can be expected, it can be suggested that the balance favours the employer’s right to monitor, rather than the employees’ right to privacy.

Speaking in broader sense about the issues of surveillance and privacy considering the ‘camera as the unblinking, unforgiving eye in our urban environment’, facial, pattern and number recognition using digital technology is being deployed increasingly to detect socially undesirable behaviour.\textsuperscript{32} Public surveillance using Closed Circuit Television (CCTV) is becoming pervasive despite the absence of empirical evidence on the effectiveness of its use as a means of crime prevention. Ultimately, the social surveillance for safety and security must be balanced with individual privacy and none should be sacrificed without justification.

\textsuperscript{30} In India, Right to Privacy is considered to be directly flowing from Art 21 of the Constitution. In number of judicial decisions, Apex Court has reiterated that Right to Privacy is one of the species of Art. 21.


\textsuperscript{32} See for e.g. Sting operations carried out by various institutions to unearth the socio-political and economical corruptions in India.
It is a matter of human choice as to which individuals or groups receive the greatest attention because of the need to select from the huge quantities of data that are being gathered. The extent of privacy protection is considered in the light of the provisions of various human right mandate, it implies that surveillance can be intrusive because of its potential for error, function creep, privacy invasion. Resources would be better devoted to combating crime in ways that are not so reliant on technology.

Individual privacy protection is an important issue in the digital age, but questions also need to be asked about whether states should have a right to privacy. As the Internet spreads, there are increasing calls for informational transparency on the part of the state, but as government services go online, whether it has right to hold that information secret?

There are strong arguments in favour of more, rather than, less state secrecy. The convergence of digital technology is providing numerous outlets for digital media. The growing capacity for information gathering and transmission means that the ‘State is paralyzed by fear’ and its response is ‘spin’. Modern democracy depends upon a ‘state of political civility’, it is becoming more and more difficult for the State to manage its relationship with the media. Individuals who embody the precepts of the State may benefit from a greater emphasis on personal autonomy, emotional release, self-evaluation, and protected communication. In developed countries like America and Continent, much emphasis are given to media management and the co-ordination of information as a result of unrelenting media coverage of the government’s actions. The argument can be leveled in favour of open debate about the feasibility of providing privacy protection for the State as an antidote to the politics of ‘spin’.

8.11 Considering Ethical values in Cyberspace

There are three main ethical positions on these issues: a utilitarian pragmatic stance based on assessments of risk and cost, a defence of human rights based on

33 The surveillance of private communication is already banned in India. Recently, the hot discussion has been taking place when allegedly, one of the ISP (Reliance communication) on the direction of one of the Political party of India, has been taping the telephonic conversation of Mr. Amar Singh, one of the leader of Samajwadi Party.


respect for human dignity, and a 'dignitarian alliance' that permits no compromise of human dignity.

It can be argued that the first position is problematic because it is subject to the erosion of rights. The second rights-based position puts respect for human dignity at the centre of ethical choices about the development of technology, indicating that individuals must have the capacity to make free and informed choices.

In the case of the 'dignitarian alliance', which is informed by a Kantian claim that human dignity has no price, developments in biotechnology are ruled out if they do not uphold a duty of self-esteem. Of the three positions, it can dictate that the first two are gaining ground.

The 'techno-regulation' is eroding the contexts in which the dignity of individual choice, responsibility and achievement are respected, with the result that technologies are being developed that treat human subjects as if they lack the capacity to choose.

8.12 Conclusion

Thus it is crystal clear that the Computer and Information technology has opened the new world for human civilization. It is tremendous potentiality, speed and power to change and capable of transformation. Its effect and impact is just beyond imagination. However, it should be noted down that ultimately, it is humanity, which has priority over the commodity; it is the man who is superior over the material. While using these machines, human instinct and human sensitivity should not be sidetracked. While switching over to new technology, we must carry the Human right book in the dark area of modernity.

Considering the evolution of Cyberspace law and the interpretative flexibility of that law from one jurisdiction to another, it is increasingly difficult to unambiguously define human rights and responsibilities in Cyberspace. The question of human rights, not as an absolute, but as a social construct is subject to interpretation in the light of changing values.

Human right is now a day taking high seat for discussion and one of the touchstone for validity and justification test for legislative piece in welfare state.
Today, human value are valued much and socio-political and economical development can be tested only after critical assessment of the position of human right in each aspect of life.

In order to have development sustainable, human rights values should be preserved, protected and promoted. Today it can be highlights the way many of the judgments and social values that appear to have achieved a consensus are subject to misapplication as we come to rely on technology to implement the law.

There is clearly a growing need for critical assessments of the 'less glamorous' aspects of Cyberspace. It is now a critical time to consider why 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 of fostering responsibility in the digital age.