Chapter 5

Social Regulation of Cyberspace

5.1 Introduction

Individuals are born into a life world that has already been organized and defined for them by their predecessors. Through socialization, individuals take for granted the existing social structures and definitions that come to constitute their natural attitudes towards the world of their everyday life. Spatial-temporal co-location of two or more individuals constitutes the condition of human contact, which shapes the form of human interaction and behaviour that in turn determines the characteristics of human relationships. A given combination of these elements makes up a given social realm which will act as regulator and then be passed on to the successors in the future realm of the life world\(^1\).

5.2 Need for social regulation

In the absence of electronic mediation, the contemporaneous life world of an individual is partitioned into two major realms: the realm of consociates where the individual interacts with others face-to-face in conditions of co-presence, and the realm of contemporaries where the individual interacts with others non-face-to-face in conditions of non-co-presence. The use of electronic communication technologies extends human perceptual reaches beyond the limits of human naked senses, resulting in the rise of a third realm – the realm of consociated contemporaries, where people interact face-to-device with each other in conditions of telecopresence\(^2\). The emergence of this social domain in cyberspace reconfigures

---

Chapter 5  

Social Regulation of Cyberspace

the structure of the life world by providing individuals with an opportunity to establish relationships in a new type of shared meaning context. In cyberspace individuals share a community of time without sharing a community of space i.e. space proximity. There is emergence of social domain in cyberspace reconfiguring the structure of the life world by creating a new spatial-temporal condition of human contact, which gives rise to a new mode of human interaction and a new form of regulation. One approach to building a secure cyberspace can be devised by developing a system based upon interpersonal relationships rather than technology. It involves devising social control from within each player rather than attempting to control them externally. A number of tools can be used for social regulation of cyberspace such as education, market forces, peer group pressure, etc.\(^3\).

5.3 Social regulation by means of Education

Many security managers believe that education and certification are important to professionals and to an organization. Education can be an effective method to help change the attitude and behavior in society. Education can increase public awareness by reinforcing safe cyberspace habits. The proper education is expected to distribute and inculcate a safe cyberspace behavior and implement a public awareness campaign. Education will also enhance six distinct meanings of social learning which are identified as\(^4\):

1. Active social mediation of individual learning, in which a person or group of persons help an individual to learn;

---


\(^4\) Available at www.itdl.org/journal/feb_06/article03.html.
2. Social mediation as participatory knowledge construction, which is learning that results from the act of participating in group effort towards learning;

3. Social mediation by cultural scaffolding, which is learning that derives from social artifacts or media;

4. The social entity as a learning system, which is learning that derives from large group or organizational participation;

5. Learning to be a social learner, learning to learn from social participation;

6. Learning social content, which is comparable to service learning or apprentice type learning in a social context, individuals learning solo, to individuals learning in groups, to individuals learning though social participation.

Cyber security awareness will help neitizens to have a complete view of cyber-crime events, and prevents offenders from lying and evading their identification.

Assigning untrained personnel to maintain security and providing no training to employees is the top error leading to severe security events and lapses. Past experience of other standards, level of documentation and standardization, degree of understanding the clauses, procedures of risk management, top management support, culture of organization, existing auditing infrastructure, and awareness of information security, education and compatibility with the existing procedures are the key factors. Thus, the responsibility to ensure secure environment should be on everyone, and the effectiveness should be highly related to the security awareness and education.

---

To increase awareness in cyberspace steps should be taken to:

- Teach the courses of information security and information ethics in elementary and junior high schools.
- Establish centre’s of excellence in research and teaching of cyber security.
- Foster more than 120 security professionals (doctoral and master students) per year.

There is need to explain people the risks as well as rewards of using online services. Organizations that are connected to the Internet must provide employees with the necessary training and information so that the employees can understand the need for cyber security. Many companies already have educational programmes for training the personnel. These programmes should be reviewed to determine whether they address online issues and if not, which need to be modified accordingly. A comprehensive corporate policy concerning the use of cyberspace is an important first step in protecting from potential misuse of cyberspace. However, a written policy is of limited value unless it is accompanied by an educational programme to instill the corporate values relating to confidentiality, mutual respect and appropriate conduct on its employees.

A well-written corporate policy regarding ethical regulation of activities in cyberspace needs to be supplemented by an educational programme to explain to employees the risks as well as the rewards of using cyberspace. Many companies already have educational programmes to train managers and others in such areas as sexual harassment, discrimination and the like. These programmes should be

---

6 Ibid.
reviewed to determine whether they address in cyberspace issues, and if not, modified accordingly. All of the ethical regulation policies in the world will not protect the company if the company itself fails to enforce those policies. As with any other employee policy, the company must take immediate steps to deal with any violation of the established cyberspace usage policy. People should learn how to be smart in operating the cyberspace.8

Remedial interventions require the human touch. A training program is probably the single, most effective method for ensuring quality and consistency in how all overseers perform their job. It not only provides an opportunity for them to share ideas and experiences, but it also instills in them the development of camaraderie and group spirit. A comprehensive program might involve periodic training sessions, role plays, on-site supervised experience, a mentor system, discussions of log excerpts from in vivo encounters with problematic users, the ongoing development of flexible but standardized interventions, and a training manual9.

### 5.4 Social Regulation by dissemination of adequate information

In knowledge society information can also act as a regulator. Many citizens contact a local police station prior to the purchase of a home in a particular neighborhood to inquire about the number of burglaries and violent crimes in the area. Just as these data provide important information for communities in the “real world”, the same is true in cyberspace. Therefore, reporting of improper conduct in cyberspace should be encouraged. For individuals and organizations to intelligently

---

8 Ibid.
assess their level of risk, agencies must provide accurate data about criminal threats. Access to reliable and timely computer crime statistics allows individuals to determine their own probability of victimization and the perception of threat level they face that helps them begin to estimate probable recovery costs. Crime statistics facilitate benchmarking and analysis of crime trends. Crime analysts use criminal statistics to spot emerging trends and unique modus operandi. Patrol officers and detectives use this data to prevent future crimes and to apprehend offenders. It is this level of understanding that would make people more cautious, more guarded, more mindful of the information they divulge to others in various transactions, and as a result, more capable of protecting the possibility of anonymity. Thus, dissemination of adequate information in cyberspace as well as in real world could help in regulation of cyberspace.

**Social Regulation by Information literacy**

Information literacy, can be defined as the process of teaching and learning about electronic technology, such as personal computers and the Internet, in order to glean and manipulate useful information from that technology. The process of teaching information literacy, if done properly, should include the teaching of information ethics; because, at their base, information literacy and information ethics are one and the same thing.

5.5 Social regulation by means of Ethics

“Be unselfish. That is the first and final commandment for those, who would be useful and happy in their usefulness. If you think of yourself only.

---

you cannot develop. Because you are choking, the source of development, which is spiritual, expansion through thought for others.”

Charles William Eliot

The law is evolving slowly to address new conflicts arising in cyberspace, but the decentralized and borderless nature of the internet creates obstacles for law and necessitates reliance on a shared sense of ethics. Ethics is the art of determining, what is right or good. It can also be defined as a general pattern or way of life, a set of rules of conduct or moral code. Ethical guidelines are based on values. Values play an important role in information technology. Values are the standards we follow in everyday life we need to adopt the right values. This is being passed on from one generation to another generation. Ethics is not an exact science, but ethical inquiry does provide a basis for choosing proper actions based on rational and sound principles, carefully reasoned arguments. Computer and information ethics are still improving and still new to us. This is a new and evolving field. Virtual communities supported by the cyberspace depend upon rules of conduct, the same way as any society. Ethical behavior arises out of the values of a community.

Nobody owns the cyberspace but everyone has his rights over it. The cyberspace is made for the public, made for everyone in short. The cyberspace not only removes communication gaps between people rather it helps us to learn and understand certain things we need or want to gain knowledge about. As technology grows, evil grows with it. People abuse information technology and create such things as viruses and spywares that infect other computers that they steal or destroy.

12 Available at thinkexist.com/quotations/you...it...only_through...you/185007.html.
the other computer. People need to have the proper state of mind or the proper morality within one self’s. There is need to put the bad side away and improve the ethical attitude of people supporting this growth. Cyberspace is a metaphor. People need to work together in order to have a better cyberspace life and realm.

A typical problem in computer ethics arises because there is a policy vacuum about how computer technology should be used. The potential applications of cyberspace appear limitless. The cyberspace is a universal tool. Indeed, the limits of computers are largely the limits of our own creativity. The logical malleability of cyberspace makes it possible for people to do a vast number of things that they were not able to do before. Since no one could do them before, the question never arose as to whether one ought to do them. In addition, because they could not be done before, no laws or standards of good practice or specific ethical rules were established to govern them. Cyberspace provides us with new capabilities and these in turn give us new choices for action. Often, either no policies for conduct in these situations exist or existing policies seem inadequate. A central task of Cyberspace ethics is to determine what we should do in such cases, that is, formulate ethical policies to guide our actions.

Cyber ethics is a special field of ethical research and application. Cyber ethics has two parts: (i) the analysis of the nature and social impact of computer technology and (ii) the corresponding formulation and justification of policies for the ethical use of such technology. Because of the global impact of cyberspace in recent years, and because of the merging of computing and communications technologies that has also recently occurred, the field of cyber ethics might be


perceived as one that is currently in a state of flux or transition or evolution. The aim of ethical regulation of cyberspace should be to enunciate and maintain high standards of ethical and professional practices in the field of cyberspace. These ethical principles can include principles relating to obligations to law, obligations to the public, obligations to the customers, etc.¹⁷

These principles be based on strong ethical basis to regulate cyberspace such as¹⁸:-

i) Neitizens will deal fairly with fellow professionals and public, giving due respect to the rights and legitimate interests of others.

ii) Neitizens will ensure that their services and promotional material does not contain anything, which may incite violence, cruelty or hatred on the basis of sexual discrimination, caste, creed or religion, etc.

iii) Neitizens shall ensure that minors are not registered by them for Internet services except with the explicit permission of their parents/guardian.

iv) Members shall be truthful in all promotional activities and publish such information, which is devoid of inaccuracies, ambiguities, exaggerations or omissions, errors about their operations, services and pricing to the customers and government/private agencies.

v) Members will design and operate their services to afford customer’s privacy and confidentiality and will post their confidentiality practices and procedures appropriately.

There should be written cyberspace usage policy based upon strong ethical principles. While the tone of a written cyberspace usage policy should reflect the

¹⁷ IGNOU, Internet Ownership and Standards and Role of ISPs, 9, (2004).
¹⁸ Ibid, at 10.
Chapter 5 Social Regulation of Cyberspace

corporate culture of the organization, the policy statement should contain at least the following ethical regulation rules\textsuperscript{19}:

- Limit personal use of corporate accounts in cyberspace.
- Limit discussions of the employer and its business in cyberspace.
- Limit the disclosure or transmission of confidential materials in cyberspace.
- Affirm the employer’s right to monitor E-mail/online usage.
- Prohibit access to or the display of illegal or objectionable materials in cyberspace.
- Prohibit any communications in cyberspace that would be illegal if communicated orally, in written form or in any form.
- Prohibit downloading of copyrighted materials (particularly computer software).

Social Organizations need to be proactive in identifying and discussing the ethical ramifications of cyberspace. At international level, UNESCO has created an Observatory on the Information Society, managed by Victor Montviloff. Its main objectives are to\textsuperscript{20}:

1. Raise awareness on the constant evolution of ethical, legal and societal challenges brought about by new technologies;
2. Provide up-to-date information on the evolution of Information Society at the national and international levels; and
3. Foster debates on related issues.

Thus by having acceptable use policies and expecting responsible ethical behavior, society can contribute to keeping cyberspace safe.  

5.6 Social regulation by market forces

Markets can be powerful regulators. In the market economy one of the main areas of interest for government has been to promote the incentives for neitizens to enter into transactions with each other. This ideology is based upon the traditional economic view that if everyone acted in their own best interests the end result would be most beneficial to society as a whole. The idea is that the individual goals of each Neitizens will collectively promote the wealth of the nation as a whole. The interacting parties whose actions do not support their original promises will develop an untrustworthy reputation and they will no longer be able to continue.

a) Regulation by trust

In this approach the regulation of cyberspace is not through law but through the market mechanisms of trust and reputation. “Companies’ economic future depends on making people feel good in the cyberspace through their reputation. The market mechanism can best be described as the importance of trust and reputation. People are not going to buy in the cyberspace if they don’t feel safe about companies’ reputation. Therefore companies value their reputations to gain trust. Trust and distrust are also seen as rational mechanisms to regulate behavior in society. Two kinds of trust may be placed in a given entity e (a person or a thing): familiarity-based trust and regularity-based trust—or, for short, “F-trust” and “R-trust”, respectively. A familiarity-based trust in e is a trust based on personal

---

familiarity with e, or on testimonial by somebody who is familiar with e, directly or indirectly, or even on some measure of the general reputation of e. A Regularity-based trust, on the other hand, is based on the recognition that e belongs to a class, or a community, that is known to exhibits a certain regularity—that is, it is known that all members of this class satisfy a certain property, or that their behavior conforms to a certain law. Both types of trust play important and complementary roles in social regulation of cyberspace.

In cyberspace there are mostly trust-based transfers. The files were transferred between friends or recommended parties rather than being left openly accessible in the cyberspace. This is a traditional method of ensuring trust. The advantage of this system is that everyone in the network can be trusted. This trust originates from the fact that they are either friends, friends of friends or share a common ideology. The side effect of this system is that the participants are a relatively closed group. Finding new partners is a more complex procedure. The disadvantage of the trusting relationship is the fact that the development of trust is complex and costly but once established, the system is cheap to maintain. Thus cyberspace can definitely be regulated not only through law but also through the market mechanisms of trust and reputation.

b) **By consumer education**

For regulation of cyberspace another social which mechanisms can be utilized by market forces to regulate cyberspace is consumer education.

---

23 Available at http://www.cs.rutgers.edu/~minsky.


Certain pre-requisites are required for regulation by consumer education: 

i) Consumers must have access to appropriate information so as to make it possible for them to become familiar with the advantages as well as disadvantages of entering into a particular transaction.

ii) Consumers must be able to contract on fair terms.

iii) Consumers’ personal data is protected as they enter into transactions.

iv) Consumers have access to adequate dispute resolution mechanisms.

v) Consumers must get information about the e-retailer, information about the product, information about the sales process, information about the terms of the contract, information as to how the consumer’s personal data will be dealt with and information about applicable dispute resolution processes.

vi) Ensures that e-retailers cannot use sales processes that confuse consumers into entering into an agreement or appearing to accept unreasonable terms.

vii) There should be a particular onus on e-retailers to avoid contracting with consumers who lack, or have limited, legal capacity.

Once all these pre-requisites are fulfilled then a properly educated and aware consumer in cyberspace would be able to adequately regulate - product quality and suitability; liability issues; exchange and refund issues; rights in the goods, etc. Thus cyberspace can definitely be regulated not only through law but also through mechanisms of consumer education.

---


27 Ibid.
5.7 Social regulation by peer groups

a) By sharing experiences

Experience has long been considered the best teacher of knowledge. Since one cannot experience everything, other people’s experiences, and hence other people, become the surrogate for knowledge. It is natural when one has a problem, be it professional or even personal, to first consult with others. In the workplace, one often consults with colleagues, who they think may have some knowledge or experience of this problem. Being able to hear their perspective can often help them understand the problem better by allowing them to appreciate the different ways in which it manifests itself. In this way, one can see which characteristics of the problem might be common with his/her situation, context or circumstance and which might be different. Social and collaborative interactions must take place in order for participants to share in the goal of identifying and responding to the problem presented to them and originating in their practice. The sharing of their experiences and interpretations of these experiences helps members of the group make sense of the problem in the context of the practice. Operational concepts and principles related to constructivism and socio-constructivism adds meaning and relevance to terms such as sense-making, multiple perspectives, authenticity, collaborative knowledge-building, and negotiation of interpretations and understandings.

b) By providing technical advice

Many technically skilled people use cyberspace, so advice and assistance from peers is easily obtained. Organizations using cyberspace have help centers

---

staffed by technical specialists who are alert to the possibilities of misuse and make efforts to regulate cyberspace to protect their organization’s resources.  

**c) By Solving Problems in Collaborative Environments (SPICE).**

Complex problems existing in cyberspace require more knowledge than any one single person can possess, and the knowledge relevant to a problem is often distributed and controversial. Rather than being a limiting factor, symmetry of ignorance can provide the foundation for social creativity. Peer group can help in improving and advancing cyber security through collaborative problem interpretation and resolution methodology. The model features a total of three steps. The first two steps are that of “Consult” followed by “Gather.” These two steps are designed to support a process of construction and reconstruction by which one can better interpret the problem, theorize about it and begin to define its contours and make them less ambiguous. Each of the three steps is followed by a process referred to in the module as that of shared reflection which is described as “a collaborative process of testing ideas, imparting knowledge, expressing opinions, describing experiences, building interpretations and asking questions.”  

Bringing different points of view together and trying to create a shared understanding among all stakeholders can lead to new insights and new ideas for proper regulation of cyberspace. Social creativity can be supported by new media that allow owners of problems to contribute to framing and solving these problems. These new media need to be designed from a meta-design perspective by creating environments in which stakeholders can act as designers and be more than consumer.  

---

29 Ibid.  
Social regulation of cyberspace by peer group will allow owners of problems to contribute to framing and solving problems of unregulated cyberspace.

d) *By providing guidelines and monitoring*

Peer group can help adapt general technical guidelines to diverse and ever-changing circumstances in the cyberspace. The peer group can also have a specific policy on monitoring online activities of employees and strong procedures to deal with any violations of the corporate policy in cyberspace.\(^31\)

e) *By social bookmarking*

Social bookmarking is the practice of saving bookmarks to a public web site and “tagging” them with keywords. Activities like social bookmarking give users the opportunity to express differing perspectives on information and resources through informal organizational structures. This process allows like-minded individuals to find one another and create new communities of users that continue to influence the ongoing evolution of folksonomies and common tags for resources. Social bookmarking creates a true web of resources and connections— one that is not limited to individuals and their folders but represents the interests and judgments of a community of users. Bringing different points of view together and trying to create a shared understanding among all stakeholders can lead to new insights, new ideas, and new artifacts which regulates cyberspace.\(^32\)

f) *By providing will to change*

Changes alone cannot change something. There should be dedication and will to change. Peer group can fight together as a team to regulate cyberspace and reinforce will to change.\(^33\)

---

\(^31\) Ibid.
\(^32\) Available at www.educause.edu/eli/
\(^33\) Ibid.
g) **By Non-cooperation**

A conscious and deliberate, partial or total, non-engagement in activities that can impede the objectives or interests of a particular person, group, institution, bureaucracy, or state system. Encompassing a large class of methods in the repertoire of non-violent direct action, non-cooperation may assume social forms (boycotts and stay-at-homes), economic forms (strikes and lockouts), and political forms (civil disobedience and mutiny). Non-cooperation rests at the core of non-violent action and is based on all systems of government relying on cooperation from their respective populations, whether through consent, acquiescence, or duress. Individuals may refuse to provide such cooperation and withdraw their support in cyberspace. Thus non-cooperation in cyberspace can provide a useful means for social regulation of cyberspace.

5.8 **Social regulation by Alternative Dispute Resolution (ADR)**

It involves wide range of procedures and approaches other than litigation that aim to identify resolutions to conflicts that will be mutually accepted by the constituent parties. ADR has evolved and been adapted to address conflicts in political and international affairs, civil and human rights, corporate and commercial interests, and community and family issues. In these areas, it is used in the processes of arbitration, conciliation, mediation, mini-trials, negotiation, peer review, and rejuvenated or reformulated endogenous means of attending to disputes. For an alternative dispute resolution mechanism to be adequate in regulation of cyberspace, it must be cost-effective, easy to understand, accessible, credible, timely, transparent to the parties, fair and capable of providing effective

---

remedies. Further, neitizens must have the right to be represented, and or assisted, by a third party.\

5.9 Social regulation through Public

“Social world” refer to a form of social organization which cannot be accurately delineated by territorial, formal, or membership boundaries. There are no particular boundaries, one could claim. The boundaries of social worlds/sub-worlds are highly fluid because they are determined by interaction and effective communication which transcend and cross over the more formal and traditional delineators of organization. Most striking “boundary” which distinguishes knowledge society as the social world is creativity. Thereby for the cyberspace it is creativity within cyberspace which is the boundary.

Cyberspace is perhaps already full of space and welcome for many social sub-worlds to grow, telling their own stories, focused on various ideas of commitment and creating different, best values and principles. Reflectiveness, justice, computer code, access to knowledge, transparency are few corrective mechanisms for the cyber world of knowledge society. Open source idea is an example of public movement. Users of a computer program with an open source code may use this program, modify it, copy the program or any portion of it, thus forming a work based on the program and distribute such modifications or work under the license terms. Therefore users learn from the program and are able to raise the level of the program and develop it. Open source idea is influencing other sectors of the market and the open content movement, originating from the United


Chapter 5 Social Regulation of Cyberspace

States is one of the examples. It is meant as the initiative of free creations and free contents” and is characterized by the will to give the society a creation. Public is able to activate corrective mechanisms and reverse everything that is not a value for the community. The primary aim of the “reflectiveness”, feature is to reverse the unfavorable trends (e.g. in law) in the cyberspace. Online self-organizing social system (OSOSS) allows large numbers of individuals to self-organize in a highly decentralized manner in order to solve problems and accomplish goals. Number of creative public initiatives has been taken to regulate cyberspace in order to protect and safeguard individual rights and public interest. Information Security is a ‘people’ issue, it depends on people. However, complicated and clever the technology gets, basic fundamental controls by the public will prevent most problems.

5.10 Social regulation by Dissemination of Good Practice

To regulate cyberspace evaluation and dissemination of good practice should be integral from the outset. Many institutions have learning development or education development units and/or centre for academic practice, which can provide support for both the evaluation of innovative ways of learning and teaching and for the dissemination of good practice. The engagement of these centre’s and departments can play an important part in successful regulation of cyberspace. Social software can support dissemination of good practice in cyberspace, reaching around the world. A group of tools has appeared in cyberspace, which can provide new ways to collaborate and communicate good practices in cyberspace. A blog is

---

probably first tool that comes to mind when thinking about social software. The blogs provide a way of reflecting on own experiences, while connecting with others facing similar opportunities and challenges. Wikis is another tool which is ideal for collaborative writing or group projects for dissemination of good practices in cyberspace. Other social tools which can prove to be useful are voice over IP and social bookmarking. The quality and reliability of VoIP has increased remarkably. Social bookmarking tag sites with keywords to organizing them searchable. Using tags agreed upon people can share and comment on good practices in cyberspace can create their own research bank of related sites. Further social networking has ability to create connections between people without regards to physical space offers some tremendous opportunities for dissemination of good practices in cyberspace. Opportunities to extend good practices in cyberspace increases as these social tools continue to integrate and expand\textsuperscript{39}.

5.11 Social regulation by self-determination and Self-regulation

Self-regulation is a private norm, i.e. that the norm is enacted by private bodies. Therefore, it stands in contrast to a public or governmental norm, which is enacted by public authorities. Self-regulation consists in the players working out and complying with rules which they themselves have formulated and of which they ensure the application. Self regulation therefore appears as a decentralized, non-hierarchical system creating its own self-imposed standards. In this model, the traditional role of the state seems to be reduced to a minimal intervention, consisting essentially in adjusting the existing legal framework to the specific character of the cyberspace\textsuperscript{40}.

a) **Forms of Self regulation**

Three possible solutions in form of self regulation have gained prominence:-

i) **Self-selection**

Self-selection means that members choose to contribute to the community entirely of their own accord, members feel no sense of being pressured to self regulate. People tend to know when and what to regulate in cyberspace. Self regulation in the cyberspace thus proceeds informally and naturally with individual’s voluntary self consent. Some measure of self-regulation in cyberspace already exists. Many technical protocols, terms and rules drafted by service providers and software designers have been posted and adopted in order to allow the regulation of cyberspace. These protocols enable to regulate across borders. Self-regulation has achieved a central role in any discussion of internet governance, to the point where it has been described as a presumptive starting point for the regulation of internet behaviour\(^4\).

ii) **Reciprocity**

One can state in cyberspace: “I help others by regulating my behavior in the expectation that they would regulate their conduct in cyberspace in return.” Cyberspace can be regulated due to a sense of reciprocity, to help others by regulating their activities in cyberspace because they had received enjoy freedom only because in some point in the past other members of cyberspace have regulated their behavior. They felt that self regulation in the cyberspace is a responsibility that they should fulfill. Reciprocity can also work the other way. Instead of regulating their behavior as a way to fulfill an obligation, some people share knowledge in the expectation of getting regulated behavior in return. This is like giving a down-payment for an expected later payback\(^2\).

---

\(^4\) Ibid.
\(^2\) Ibid.
iii) A non-competitive environment

The very nature of the cyberspace also plays an important role in supporting and sustaining the online community of practice. Many neitizens are more willing to regulate their behavior in cyberspace due to the non-competitive environment afforded by the online communication medium that brings people from different organizations together.\(^\text{43}\)

b) Motivation for Self regulation

Self regulation involves intrinsically-motivated behavior or extrinsic motivation. Two basic innate needs that are relevant in accounting for intrinsically-motivated behaviors: a) the need for autonomy i.e. when people’s intrinsic need to be self-determining is met—that is, when there is an internal perceived locus of causality, intrinsic motivation for the behavior concerned is supported and can be enhanced; ii.) The need for competence i.e. when people’s intrinsic need to be competent and to master optimal challenges are met (within the context of some self-determination)—or, more specifically, when there is perceived competence— intrinsic motivation for the behavior concerned is supported and can be enhanced.

Not all activities are inherently interesting; hence there is a place for extrinsic motivation. Extrinsic motivation can be a continuum of autonomy involved\(^\text{44}\).

There are different degrees of autonomy with respect to extrinsic motivation:

i. external regulation – the behaviour is controlled by external demands or externally-imposed rewards

ii. introjected regulation – the behaviour is driven by ego or self-esteem

\(^{43}\) Ibid.
\(^{44}\) Ibid.
iii. **identified regulation** – the person has identified with the goals and values of the regulated activity and hence accepts the external regulation

iv. **integrated regulation** – the identified regulation is fully internalized such that the extrinsically-motivated behavior becomes a self-determined one, the activity is now volitional and valued by the self\(^45\).

c) **Implementation of self regulation**

Self regulation is not limited to very isolated norms but more and more encompasses a set of structured norms included within codes of conduct or codes of practices and provides not only the content but also the means to enforce these rules. The actors themselves have developed means to ensure that the self-regulatory code passes from the letter to the act. The typical sanctions in the regulation of a network are such as *disconnection* and *flaming*, *hot lines* created by certain codes of conduct to enable the condemnation of activities contrary to that code, *quality labelling* mechanisms inform the user of the quality of the service being offered. ADR mechanisms such as *virtual magistrates*, online arbitrators or mediators who are authorized to adjudicate conflicts arising out of network are also available. Private regulatory sources establish their own mechanisms for expressing the rules, controlling their application and finally for sanctioning violations, in certain cases, the sanctions are imposed by their own ‘magistrates’\(^46\).

Overseas, promoting self regulation and international cooperation is popular. In Germany there are proposals to extend existing self-policing arrangements for the press and broadcasting to the cyberspace. There is need for cooperation from the industry in establishing a “fully functioning system of self-

---

\(^45\) Available at www.edublog.net/astinus/mt/files/docs/apera%20paper-chongeddy.pdf.

regulation” with Internet service providers and users establishing representative bodies. There should also be greater cooperation between police and self-regulatory bodies.47

5.12 Social regulation by Co-regulation

It is the ‘effective mix’ between self-regulation and public intervention. The main idea is that it would be impossible to regulate the cyberspace effectively if private and public bodies do not combine their efforts simultaneously. Self-regulation is no longer solely in the hands of the private sector. Public regulation is fixing the context of this self-regulation and the conditions of self-regulation legitimacy that must be set up, drafted, implemented and evaluated by all actors interested in this regulation. Thus the industry will have to work together with representatives of consumers, civil liberties’ associations, privacy authorities and definitively with official authorities in charge of the prosecution of crimes.48

Trends in co-regulation

a) The initial trend (before 1998): supporting private sector leadership

The various industries concerned had a key role to play in developing and implementing solutions to the problem of protecting minors and human dignity… The main tasks which industry worked on were:

• drawing up a code of conduct…

• identifying areas where there may be a need for common standards on the labeling material;

• promoting standard systems\textsuperscript{49}.


This recommended:

• the encouragement of the participation of relevant parties (such as users, consumers, business and public authorities);

• the establishment of a national framework for self-regulation by operators of online services\textsuperscript{50}.

\textit{c) Latest trend (from 2000):}

It is marked by giving more investigatory power to the state but limiting Internet provider liability. Self-regulation is viewed as a form of \textit{coregulation}, with greater state involvement – so that self-regulation is viewed as involving either the state delegating authority to regulate or maintaining a degree of control over the operation of the self-regulatory process\textsuperscript{51}. Finally, in between those extremes the third approach emerging is \textit{hybrid arrangement} – that is to say, something which combines elements of both state and self-regulation to achieve a particular goal which neither individually could reach\textsuperscript{52}.

\section*{5.13 Role of religion in Social regulation}

Religion can also play a role in regulation of cyberspace. Each religion has a code of moral behavior and expression to which its believers subscribe. While within a pluralistic society one set of believers may be prevented from making the entire population follow their morality, they are usually able to encourage it among

\textsuperscript{49} Ibid.
\textsuperscript{50} Ibid.
\textsuperscript{51} Ibid.
their own ranks through social networks and regular religious gatherings which enclose individual believers within a supportive environment.\[^{53}\]

Religious tendencies towards improvement in cyberspace can be fostered through conscientious human endeavor. This implies that each religion must be included, not just to individual needs, but for the assets which they can offer to regulate of cyberspace. There is need to establish trust and cohesiveness across the various religions and institutions run by religious communities in India. Conscientiousness, religious assumptions and beliefs, and social conditions can affect behavior and attitude towards work, in general, and cyber security awareness, in particular. Following steps can be undertaken for better regulation of cyberspace\[^{54}\]:

- Establish cyber security policies and procedures. Policies need to be tailored to religious communities and more generally the India’s environment. They also need to be achievable, clear, and easy-to-understand.

- There is need to campaign cyber security awareness best practices and advertise cyber security training sessions and materials. It is also important that these messages reach as many users as possible and allow enough time for users to participate.

- Train users among various religious communities on cyber security best practices to increase their awareness. Training should be regular. Basic level training should be mandatory for all users.

- It is important to monitor performance, and advertise reward and punishment of cyber conduct or misconduct in various religious communities.

\[^{54}\] Ibid.
• It is highly expected that with time, use, and maturity, the status of cyber security awareness will significantly improve in the higher education sector among various religious communities in India.

While it is important to establish cyber security awareness in higher education, a viable system of higher education among various religious communities is a definite pre-requisite\(^{55}\).

The India has passed Information Technology Act but the government is apparently content to allow the trust services among religious communities to regulate itself rather than to bring the religious communities under direct legislative control. Consequently there is need to establish standards for supervision and accreditation schemes by not-for-profit organisations\(^{56}\).

### 5.14 Social regulation through Cameralism

The name Cameralism denotes a school of thinkers developed in the German principalities. They called themselves cameralists, since they formed chambers of advisers to local rulers. Their task was to devise the policies which would guide the ruler in economic policies in particular. First, the cameralists embraced an empirical belief that a growing population is beneficial, owing to the increasingly fine division of labor that it makes possible. This is similar to the present-day belief that the expansion of cyberspace is apt to stimulate the ‘new economy’, as well as the development of new forms of property and new rules of behavior within virtual communities. Second, such categories that cameralists dealt


with as principal, agent and property are identifiable now in the form of shareholders, corporate management and intangible assets exist in cyberspace. Third, the cameralists developed a system of Polizeiwissenschaft, which would account for the maintaining of reliable standards, order and public security which can be applied to regulate cyberspace.

5.15 Social Regulation through taskforce

To monitoring cyberspace for its proper regulation taskforce can be constituted by the society having representatives from private and public sector. Such taskforce can discharge important responsibilities in regulation of cyberspace such as:

- Developing a comprehensive national plan for securing the key resources and critical infrastructure;
- Providing crisis management in response to attacks on critical information systems;
- Providing technical assistance to the private sector and other government entities with respect to emergency recovery plans for failures of critical information systems;
- Coordinating with other agencies of the government to provide specific warning information and advice about appropriate protective measures and countermeasures to state, local, and nongovernmental organizations including the private sector, academia, and the public;

---

• Performing and funding research and development along with other agencies that will lead to new scientific understanding and technologies in support of homeland security.

Consistent with these responsibilities, taskforce will become a center of excellence for cyber security and provide a focal point for outreach to state, local, and non-governmental organizations including the private sector, academia, and the public.\textsuperscript{60}

In India, The Ministry of Communications & Information Technology has issued security guidelines to all ministries and government departments asking them to set up 24 X 7 cyber control rooms, implement information security best practices, deploy information security experts and formulate their own information security policies. The National Crisis Management Committee headed by the Cabinet Secretary also monitors all national level cyber crisis. Thus the Government of India is reportedly developing a full fledged Crisis Management Plan for countering cyber attacks with help of experts from the society.\textsuperscript{61}

### 5.16 Social Regulation: International Perspective

Cyberspace is better served by social regulation. The government should only step in when absolutely necessary. The primary problem in regulation of cyberspace is that it is difficult to get various countries to agree on a set of universal regulations. Therefore even developed countries are trying to evolve social mechanisms to regulate cyberspace.\textsuperscript{62}

\textsuperscript{60} Ibid.


a) Models of Social regulation in United States (US)

US approach to the social regulation of cyberspace emerges from a distinctive social and cultural experience. This experience reflects, at different historical moments, divergent concepts of the individual and fundamental rights, the nature of civil society, and the legitimate scope of state power with respect to each. These social, political, and cultural conceptions can be organized into three traditions of regulation that are tied to separate American theories of the individual, society, and the state.

i) US libertarian model

The libertarian vision of the cyberspace and communications technology derives from a concept of society without the state. In the libertarian view of communication and regulation, the information networks of a society are open and non-proprietary, with strict constraints placed upon state intervention on any grounds, even for entirely rational aims such as the protection of minors. From the standpoint of a minimal state tradition that libertarian conceptions of information networks represent, the rules of conduct within the system are only regarded as legitimate if they evolve from consensus among users and participants, with conflicts resolved largely through negotiation and dispute resolution. Thus the libertarian view of society and communication is averse to control, regulation or monopolization in information space, and supportive of unobstructed processes of interaction among individuals. New media digital and wireless technologies in a networked environment thus become the new frontier of a different space that must be carved and structured by those who utilize and exploit it, and not by institutional authorities, proprietary regimes, traditions of law, or the coercion of the state.

63 Ibid.
64 Ibid, at 70.
ii) US public interest model

Rather than being founded on a diminished belief in market forces, it is founded on the reverse: a faith that perfect markets can, in fact, be achieved by rational regulation. The public interest model assumes that markets can be made to behave. The public interest model, too, has roots in the American experience of social and political tensions between the rights of individuals and the boundaries of government. However, the public interest model resolves this tension by arguing for, rather than against, the application of state power to protect individuals from an even greater social threat thought to reside in unaccountable structures of the marketplace. To assure the structures of a functioning market in communications, whereby innumerable producers and consumers of a commodity or service are finely balanced so that no single market participant dominates, the tradition applies a complex body of mechanisms. These include: competition law, access rules, universal service in areas of essential need, educational applications and subsidies, government investment in scientific and technological research, privacy protection and protection of minors, unbundling, interconnection, and interoperability requirements, ‘fair use’ and a limited monopoly principle in intellectual property laws, and safety, standards, tariff, and fair trade practices, among many other public interest regulations.65.

iii) US liberal market model

It emphasizes contractual rights and proprietary freedoms for market participants. The principles require a minimum of state intervention in market relations between producers, consumers and distributors of goods and services. The liberal market model argues for a more powerful legal regime guaranteeing contractual and proprietary rights in the marketplace.66.

65 Ibid, at 71.
66 Ibid, at 72.


b) **International perspective on self regulation/co-regulation**

The ‘Internet Content Summit’ was organized in Munich on 9-11 September 1999 and funded by the Bertelsmann Foundation in cooperation with Internet Content Rating for Europe. At this Summit, the Bertelsmann Foundation presented the “Memorandum on Self-Regulation”. This Memorandum was the central pillar of the Internet Content Summit. It contains key recommendations for the Internet industry, policy makers, law enforcement authorities and cyberspace users. These recommendations are allegedly based on reports by leading experts from four universities, around the world, and on the Internet User Survey, that was carried out in Australia, Germany and the United States. However, in a report prepared for the OECD it has been accepted, “while there is a broad consensus that self regulation of the Internet is critical to its future growth, there is little consensus about how to achieve and to implement a self-regulatory regime.” Therefore the OECD Ministerial Conference on Electronic Commerce, held in Ottawa on 7-9 October 1998, discussed in depth the idea of combining the two previous regulatory approaches in a co-regulatory effort of both private as well as public partners. Still more recently, the World Summit for Regulators pleaded clearly for a co-regulation.67

c) **International perspective on taskforce**

European Commission (EU) has proposed the establishment of a cyber security taskforce as part of its network security proposal to be rolled out to all the member European states which will consist of representatives from member states

---

67 Ibid.
and experts from industry working closely with the private sector\textsuperscript{68}. Cyber security taskforce will not be law enforcement but an office that will facilitate communication across the EU about who to call during a security crisis. Security in cyberspace is a cross-border issue and there is not enough communication about security. This is where the cyber security taskforce will come in picture.

d) **Development of hotlines for illegal content**

Hotlines for reporting illegal Internet content has been promoted by the European Union’s Action Plan and the UK’s Internet Watch Foundation (IWF) represents one of the earliest examples of such an hotline. The IWF acts as a hotline for reporting illegal content, and this involves mainly child pornography. The IWF, as an industry based self-regulatory body, was announced in September 1996 (supported by the UK Government). The organization is a private body financed by the Internet Service Providers and it is not an accountable public body. Thus a new partnership approach between the Internet Service Providers and the law enforcement agencies can be seen as the best way to address criminal content and criminal activity over the cyberspace together with the improvement of law enforcement techniques in relation to cyberspace -related crimes\textsuperscript{69}.

5.17 Conclusion

To conclude, making cyberspace secure is a difficult challenge that requires coordinated and focused effort from our entire society - the central government, state governments, the private sector, academicians, industry and the people.


Society is not the only source of constraints on behavior in cyberspace: such behavior might also be constrained by law, social norms and practices, or even by the very architecture of cyberspace itself. But while each of these latter factors is contingent and hence can change over time, there are certain basic social principles that remain fundamental. These principles developed by the society about policing cyberspace should guide and direct the ways in which code, laws, the market, and social norms exercise their regulatory power\textsuperscript{70}. While regulating cyberspace more emphasis be placed on social-regulation, with government stepping in very carefully and only when necessary and second, to suggest that social -regulation is best accomplished by utilizing the end-to-end nature of the cyberspace. Neitizens need to examine their activities from an social and ethical perspective to make adjustments accordingly. People who use the cyberspace need to accept some responsibility to keep their information private and secure\textsuperscript{71}. There is a need to evolve an elaborate social mechanism to regulate cyberspace.

In order for an information and knowledge society to emerge and flourish, several social and political preconditions must be met. These preconditions includes: (1) a functioning public sphere (print, electronic, digital, broadband) open to broad participation and deliberative engagement among major social groups; (2) a percentage of the public communications system capacity reserved for non-commercial exploitation in order to strengthen the foundations of civil society and associational development; (3) guarantees of citizens’ information rights through freedom of information laws, government transparency, and public service obligations for information providers to serve the public-opinion formation process; and (4) access to knowledge, information and an educational system that

\textsuperscript{70} K.E.Himma, Ethics and Information Technology, 69 (2004).
cultivates independent judgment instead of rote learning. Need for a fundamental shift in approach to regulation in cyberspace that may offer a more effective design for its democratic and social development. For the foreseeable future each and every member of the society can make contributions to secure cyberspace. The society needs to be best equipped and structured to respond to an evolving cyber threat. Public-private engagement can play a key component to secure cyberspace. This is true for several reasons. Public-private partnerships can usefully confront coordination problems. They can significantly enhance information exchange and cooperation. Public-private engagement will take a variety of forms and will address awareness, training, technological improvements, vulnerability remediation, and recovery operations. Social regulation can become primary means of control of cyberspace.

A certain level of social responsibility is associated with use of cyberspace. There is nothing guaranteed in trying to secure cyberspace. There are always new bugs, new forms of attack, and new opportunities for breaches that arise from human error. However, a set of best practices with diligence and care, can improve chances of operating in cyberspace securely. In cyberspace there is movement from anomy (non-regulation by others or the self) to heteronomy (regulation by others) to autonomy (self-regulation). Social life is necessary condition for the development of logic, and that ‘social life transforms the very nature of the individual’. If cyberspace is not socially regulated then the cyberspace will become either an anarchic wasteland, or a super regulated government tool without the freedom that the cyberspace needs to grow and improve. Self regulation has not

---

worked\textsuperscript{73}. A cohesive network of socially interacting agents can create a highly robust and adaptive defence system\textsuperscript{74}. Further there is need to develop global social regulations so as to increase its horizon for regulation of cyberspace worldwide.