A Comparative Study of Regulating the Filtering of Cyberspace in the US, the EU and China; Proposals for Policymaking in Iran

Hassan Bashir
Mohammad Sadegh Nasrollahi *

(Received 01 August 2017; accepted 21 October 2017)

Abstract
The crucial role of cyberspace attracted the special attention of the governments in different countries, which consider it both as a challenge and an opportunity. One of the key policies and preventive measures adopted concerning the challenges posed by the cyberspace is it regulation. In fact, there are only a few states have not taken any steps in regulating their cyberspace. This paper seeks to demonstrate a set of policy proposals for the Islamic Republic of Iran through the study of three leading but different precedents in regulating the cyberspace, including the United States, the European Union, and China. This study employs a descriptive-analytical model, which recommends placing the main investment in and concentration on the final user, employing economic strategies, special attention to governmental and public institutions, prioritizing content removal over blocking, negotiating an agreement with Foreign Service providers, drafting a content rating system, and using international capacities for cooperation. Accordingly, the final policy proposals for the Islamic Republic of Iran would be decentralization, user-oriented decisions, prioritizing removal over blocking, and monitoring over filtering.

Keywords: cyberspace, filtering, internet, monitoring, regulating, regulation, surveillance, virtual space.

Hassan Bashir: Professor, Imam Sadiq University, Tehran, Iran- Email: bashir@isu.ac.ir
Mohammad Sadegh Nasrollahi: (corresponding author). Assistant Professor, Imam Sadiq University, Tehran, Iran- Email: m.nasrollahi@isu.ac.ir

Introduction

To tackle political, security, economic, legal, cultural and social concerns, all governments place cyberspace policy-making within their agenda. This is indeed both a unique opportunity and a challenge for all countries. In one categorization, the general policies dominating the cyberspace could be divided into imperative and preventive. For instance, improving internet infrastructure is imperative, while imposing punitive policies is preventive.

Filtering is one of the preventive policies pursued by governments based on their value structures and meant to purify the cyberspace. A 2008 study by Ronald Deibert and his colleagues entitled "Access Denied, Practice and Policy of Global Internet Filtering" indicates that there are few countries without any policy in their agenda. What differentiates the countries and their experience in regulating cyberspace is both the limit and method of regulation. This paper offers a comparative analysis of three leading cases in the cyberspace that is the United States, the European Union, and China. Other than the leading role of these countries in cyberspace, this selection is based on diversity in the regulatory systems. In other words, the choice of case studies was based on their policy-making approaches in self-regulation, co-regulation and state regulation, so that the comparison would be valid and make sense. The analogy could put forth the effective alternative options as a package of proposals for the Islamic Republic of Iran's cyberspace regulation policies.

To gain such an objective, the research tries to initially map out the structure within which it has been conducted. Afterwards, the cyberspace regulation systems in the US, the EU and China will be elucidated, while in the conclusion, the three systems will be compared and practical proposals, to be used in Iran, will be offered.

1. The Theoretical Framework of the Comparative Study

The results of some studies indicate that regulation systems in the above-mentioned cases can be analyzed from the following three perspectives:

1. The policymaking structure
2. The legal system
3. The Technical-executive order.

Based on these three aspects, the paper analyzes the ruling legal structure, the laws and orders and the processes through which regulations are implemented. Here, the three issues are being fully explained.

1.1. Structure of Regulation Systems

The term "regulation" has found a variety of definitions and equivalents in Farsi, which could cover a variety of concepts, including policymaking,

agenda setting, legal supervision, ordering, setting up, etc. which indicates the widespread and different uses of the word. The same holds true when the term is applied in technical contexts. Referring to valid English dictionaries confirms the extensive applications and uses of the word, ranging from a thermometer to a country's constitution.

Oxford Dictionary defines regulation as:

1. A rule or directive made and maintained by an authority, 2. The action or process of regulating or being regulated, 3. Person or organization that officially supervises an area of trade or industry to make sure that the rules are properly implemented (Wehmeier, 2005, p. 1275).

Similarly, *Webster* stresses two major meanings: an authoritative rule dealing with details or procedure and a rule or order issued by an executive authority or regulatory agency of a government and having the force of law (Costello, 1992, p. 1135). The four key responses in Longman are the following: an official rule or order, control over something, especially by rules, a person who controls the implementation of rules, a tool used to control temperature, speed, etc. (Summers, 2003, p. 1382). This last definition almost offers the same equivalents, while also refers to a physical tool rather than a social one.

As a result, the definitions offered for the term "regulation" allude to a wide range of concepts which can be categorized into the following binaries:

- Drafting and ratification of a legal text or a legal text itself? (Process-product)
- Does it refer to law as a general rule (issued by any authority) or is it an active for special purposes (from the executive branch)? (Legislation-execution)
- Is it about supervising the implementation or is it implementation itself?
- Is control merely a passive process or does it also involve change as an active part? (Passive-active)
- Is it a person in charge of control or is it an organization? (Individual-collective)
- Is it exclusive to supervising industrial and trade organizations, or does it cover a more general category including all organizations? (Economic-beyondeconomic)

In general, "regulation" in this paper is the legal structure in charge of creating and enforcing order on a special field, whose decisions are obligatory to follow by the players in the field. Those decisions could include directives, tariffs, supervising the implementation, etc. The three

major aspects of the nature of regulating structure, as far as this paper is concerned, are self-regulation, co-regulation, and state regulation. More specifically, the regulating system could follow three major patterns as Ansari (2011, pp. 98-99) illustrates:

1. Self-regulation (regulating by the individual)
2. State regulation (enforced by the government)
3. Co-regulation (enforcing a shared regulating system).

The logic behind the categorization derives from the nature of the structure that is, whether it is private or governmental. Basically, such a nature is limited to the following three forms: the regulations are set, ratified and implemented by the private sector and people, by the government, or by a combination of both the private sector and the state.

1.2. Legal System

The concept of the legal system in this paper refers to all legal documents including policies, laws, and rules which are ratified and implemented in regulating the cyberspace. In this regard, the paper is to offer a comprehensive picture of legal systems applied in the three case studies.

1.3. Technical-Executive System

The technical structure is a series of ideas and measures which are implemented at the executive level as a consequence of the policies and rules set by officials with regulation purposes.

2. Research Method

This research has been conducted with a document study approach through a library or descriptive analysis method. In this regard, the effort is to collect and analyze the legal documents of the countries and related sectors in accordance with the research question.

3. The United States of America

One must acknowledge the fact that the US was the country which founded the World Wide Web. In the same field, the US is still the pioneer in the infrastructure, service providing, content as well as user population. This has helped the country to access more options when it comes to cyberspace supervision and control. One clear example of the American influence and power in this regard is its possession and control over domain names. Additionally, is the widespread leadership of the online content, redirecting through offering cyberspace to other countries, also known as hosting services, which gives the US the advantage of path finding (Jalali Farahani, 2007, p. 21).

3.1. Regulation System

The cyberspace regulation system employed in the US is referred to as a self-regulating one which sets the policy itself (Frybman et al., 2008, p. 173). In other words, the private sector plays a key role in supervising and regulating the American cyberspace. The most active groups in such area are companies producing "parental control" software and access providers, which offer services to users in an optional manner.

In the US, cyberspace state control is mainly and only focused on schools and libraries (Deibert et al., 2008, p. 226) and is best manifested in CIPA (Children's Internet Protection Act). Another clear example of self-regulation is the Digital Millennium Copyright Act (DMCA), which has been signed based on an agreement between copyright owners and representatives from electronic businesses, both from the private sector. Yet, in the case of the US, the self-regulation system does not deny the role played by the government in control and supervisions. In fact, a minimum minimal and emergency presence of the state is still visible. This will be later discussed in detail.

3.2. Legal System

Since 1996, the US has ratified five different internet regulation acts (some of which have been revoked by either individual courts or the Supreme Court. This will be explained later). The acts, in order of subject and ratification time, are listed below:

- Communications Decency Act (CDA)-1996
- Child Online Protection Act (COPA)-1998
- Child Internet Protection Act (CIPA)-2000
- Digital Millennium Copyright Act (DMCA)-1998
- USA Patriot Act-2001.

The paper elaborates on Details of all those acts later.

3.2.1. Communications Decency Act (CDA)

As part of the distant communications law (Deibert et al., 2008, p. 228), the CDA is considered as Congress' first measure, taken in 1996, aimed at regulating children's access to explicit sexual content on the internet (Jalali Farahani, 2007, p. 26).

The act stipulates that providing "indecent material" and "patently offensive content" to individuals below the age of 18 is regarded as an offense. Meanwhile, a "safe harbor" has been given to internet service providers to create technical barriers for children's access to such material (Deibert et al., 2008, pp. 228-229). Simply, the Communications Decency Act criminalizes any conscious transfer of indecent content or

message to underage users. There is also strong support and justification for people who, based on their goodwill, limit children's access to the adult material (Deibert et al., 2008, p. 229).

However, the law was annulled by the US Supreme Court in 1997 (Deibert et al., 2008, p. 229). The court recognized that such terms as "indecent" and others used by the act were general and vague, thus declaring the act as violating the First Amendment. The only remaining binding portion of the act is the section which allows service providers to voluntarily introduce some provisions which could restrict access to content that is obscene, sensual, disgusting, graphic and violent. This makes the provider exempt from prosecution (Amn Afzar Gostar Sharif Service Provider, 2008, Chapter 1. Vol. 2. Report 2, p. 43).

3.2.2. Child Online Protection Act (COPA)

Reacting to the Supreme Court's decision to revoke the Communications Decency Act (CDA), US lawmakers introduced a new bill: The Child Online Protection Act (COPA) (Balkin et al., 1999, p. 2; Deibert et al., 2008, p. 229). The legislation aimed at regulating children's access to explicit sexual material on the internet and followed the cancelation of the CDA by the Supreme Court. It was ratified by Congress and made into law in October 1998.

COPA stipulates that the service providers report to authorities any material containing child pornography. Failure to do so results in a punishment of 50,000 dollars and a second failure would double the fine (Frybman et al., 2008, p. 176). The law also proposes connection and synchronization of the online account of parents to their credit cards, their user IDs, passwords and a digital certificate that could verify the user's age and limit access to potentially damaging content for the ones below the legal age (Ameli, 2011, p. 346).

However, the story of COPA was similar to that of the CDA. Initially, a local Eastern Pennsylvania court placed a temporary ban on it and later in February 1999, it was completely annulled (Wang cited by Ameli, 2011, p. 345).

3.2.3. Child Internet Protection Act (CIPA)

The legislation was approved by Congress in December 2000 and came into force as of April 21, 2001. The law obliged all state schools and libraries, which are funded by the federal budget, to use the E-Rate software on their internet access. As part of a comprehensive plan to guarantee healthy internet use for children, the software versions were employed by the Federal Communications Committee, the Education

Department and the Institute for Museum and Library Services. The plan includes technical supports that impose restrictions on users under the age of 17 in their online activities, which fully bans access to obscene pictures, child pornography as well as extremely dangerous material for minors. To achieve this goal, schools and libraries are required to be equipped with computers that have the preventive technical support. Still, the same law allowed a lift of the restrictions when parents are the users (Jalali Farahani, 2007, pp. 27-28).

Meanwhile, the law permits principals and librarians to temporarily deactivate the regulatory systems for adults and children in special cases for research or other permissible purposes (Deibert et al., 2008, p. 230). Libraries which follow the rule are all equipped with the Web Sense software. Although all libraries can use their own regulation settings in the system, they mainly heed recommendations by the consortium (Amn Afzar Gostar Sharif Service Provider, 2008, Chapter 1. Vol. 2. Report 2: 30). In practice, a small number of the libraries and schools refused to receive financial support. Provided that most of libraries and schools are dependent on the federal budget, it had been decided to install the regulator software (Deibert, et al., 2008, p. 229).

The American Civil Liberties Union and the American Library Association filed a lawsuit with the Supreme Court, claiming that the law was in breach of the First Amendment. The court, nevertheless, turned down the case. The Child Internet Protection Act, indeed, encourages some integration and involvement with the service providers and other internet companies. Moreover, CIPA helps them play a role by offering information to state officials while also taking some law enforcement as they are authorized to directly restrict access to controversial content (Frybman et al., 2008, p. 176).

3.2.4. Digital Millennium Copyright Act (DMCA)

When it comes to copyright laws, Congress specifies clear responsibilities for service providers. In 1998, the Digital Millennium Copyright Act (DMCA) incorporated into the Copyright Directive the 1989 Washington Treaty that was signed between intellectual property owners and representatives of electronic businesses and criminalized the circumvention of all literary and artistic properties.

The act exempts the service providers from liability when they are unaware of hosting information which violates the copyright of the owners, not beneficiary to the dissemination of the content, or is in breach of intellectual property laws. If the copyright owner reports the breach, the service providers face the deadline to either remove/

make the content inaccessible within 10 days or pay the compensation. In this case, the content publisher must be notified for content removal/ inaccessibility. Then the publisher would have a chance to issue a warning to the provider for removing the material. Afterwards, the service provider shall inform the intellectual property plaintiff concerning re-publishing the disputed content. However, this would not be the case if a lawsuit was filed against the person accused of copyright violation and demands a temporary court ruling (Frybman et al., 2008, p. 177).

3.2.5. USA Patriot Act

In the wake of the September 11 attacks, the US government policy suddenly shifted from "Cyber Democracy" to "Cyber Security". 40 days into the attacks, October 26, 2001, the extensive and controversial Patriot Act was ratified allowing the FBI and the NSA to breach the privacy of users worldwide, and access and record their data. Subsequently, agents have been granted the authority to install so-called black boxes on the servers of the service providers. The aim is to fully track all online communication with residents of "hostile" nations and in-depth analysis to higher authorities (Jalali Farahani, 2007, p. 22).

Furthermore, in cases of good will, the act allows the service providers to leak information to the local or federal authorities if they find the case to be an emergency, or the information can save lives, or prevent serious damage to someone's health. They have the permission to do so in such cases, while facing no legal pursuit. In fact, that's where the service providers are immune from prosecution and protected against claims of breach of privacy laws. Providers are additionally encouraged to cooperate and act as law enforcement authorities (Frybman et al., 2008, p. 176).

3.3. Technical-Executive System

The United States is a progressive pioneer of internet regulation systems and the related software versions. Although the country applies those systems in a very limited manner, its products are being vastly used across the world (Amn Afzar Gostar Sharif Service Provider, 2008, Chapter 1. Vol. 2. Report 2, p. 14). Interestingly, the American regulatory system is more concerned with content removal than blockade (Deibert et al, 2008, p. 226). What makes removal a better option is that it leaves no space for circumvention. For a government to do so, it requires to be equipped with advanced infrastructure, especially hosting provisions.

There are two general technical regulation strategies on the internet that are employed in the US. They are divided into the ones for the final

user and the ones for the service providers. Measures in the first strategy are either technically preventive or socially preventive. There is a large number of software developers in the US dedicated to techniques of parental control over children's internet activities. The strategies for the final users are commonly proven to be more workable than regulation methods applied by service providers. The same level of attention has also been paid to social preventive strategies. For the latter strategy, the necessary training and awareness on internet threats and challenges is offered to children and young adults. The social preventive strategies balance the judgmental views toward the new generations that is held by the parents with less interaction with cyberspace (Jalali Farahani, 2007, Vol. 2: 23 and 24).

The three major techniques applied by the service providers are: a) enforcing the producers of obscene material to use XXX in their domain addresses, b) expanding top-level "kids" domains, and c) developing techniques for age verification conditions (Jalali Farahani, 2007, Vol. 2: 25).

4. European Union

The European Union is a bloc of advanced countries in the field of cyberspace and the internet. While making progress in both software and hardware technology, the EU faces its own threats, challenges and offences which the internet use might be associated with. This has made internet regulation a widespread and common issue in the EU making it no longer an exception (Deibert, et al., 2008, 186). In the following, a brief glance is taken at the EU's plans and efforts made to regulate the cyberspace.

4.1. Regulation System

The European Union is known as a united bloc of countries with common policy-making strategies. It's a zone where both states and the private sector are putting serious work into the internet regulation. In this regard, the member states have come to the common conclusion that enabling the final users by raising awareness, training, cautioning, and equipping them with the latest preventive hardware and software technology is way more workable than improving the cyberspace infrastructure (Jalali Farahani, 2007, Vol. 3: 28).

4.2. Legal System

A shared regional policy in the European Union is limiting the activities of the access provider, as part of which the "Electronic Commerce

Directive" was ratified in 2008 (Deibert et al., 2008, p. 187). According to the directive:

- Access providers have been forbidden from controlling content through service providing (Deibert et al., 2008, p. 188).
- Since access providers are merely conduits, they face no responsibility regarding the information transferred in their networks as long as they do not initiate the transfer, choose, correct the content, or set the target audience (Deibert et al., 2008, p. 187).
- In the European internet regulation, the case of hosting servers is different from that of the access providers. According to the same directive, they are not held accountable unless they have knowledge about illegal activities. They are, however, obliged to immediately remove the content upon reporting (article 14 of the directive) (Deibert et al., 2008, p. 188; Frybman et al., 2008, p. 179).
- Alongside the servers' hosts and access providers, there is a third entity involved in content control. This third party informs users about indecent internet material, giving "hotlines" to both individual, and organizational users. Those firms are responsible for standardizing the cautioning, official response procedures, and play a crucial role in a close and quick oversight of the activities of the internet service providers. Such companies are significantly prompt in their responses to complaints and controversial issues raised by the users. One major element in the standardized online forms they offer is the verification process and the emphasis on the fact that their warning needs to be valid and honest and that they would have suffered the legal challenges if they report on baseless grounds (Frybman et al., 2008, p. 180).

Although the above directive enforced in the European Union eases the responsibilities faced by the service providers, it offers fewer benefits to them at the same time when compared to the Communications Act in the U.S. It also allows more state interference, prepares more ground for, and offers more support to professional entities which are trusted in internet content control (Frybman et al., 2008, p. 178). The directive does not force the service providers to control the information, which is recorded/transferred in their networks, or to actively monitor possible illegal activities there. Still, EU member states have the authority to oblige the service providers into reporting on illegal information and other violations conveyed to them through their clients and reveal the identities of the violators to the state as well. National courts and state officials are also allowed to force the internet service providers into

restricting access to or totally removing material, which is viewed as harmful, illegal or in breach of other people's rights (Frybman et al., 2008, pp. 178-179).

4.3. Technical-Executive System

From a macroscopic perspective, state regulation of the internet includes reducing the illegal content, blocking it, as well as purifying the results offered when such content is searched (Deibert et al., 2008, p. 186). In April 1996, the European Council requested the European Commission to draft "a summary of problems posed by the rapid development of the Internet," and assess the need for policymaking. The commission reported "Illegal and Harmful Content on the Internet" as well as "The Protection of Minors and Human Dignity in Audiovisual Services." Based on these reports, the Commission offered "a common framework for self-regulation (of the Internet) at the European level," and devised an "Action Plan on Promoting Safe Use of the Internet." The package, ratified on January 25, 1999, became operational in 2002 and was enforced until 2005 (Amn Afzar Gostar Sharif Service Provider, 2008, Chapter 1. Vol. 2. Report 2, p. 38; Deibert et al., 2008, p. 187). The 25-million-euro project proved a success, thus a second version was also developed, unveiled, and enforced between 2005 and 2008 (Ameli, 2011, p. 356). The budget allocated to the second phase was around 45 million euros (Amn Afzar Gostar Sharif Service Provider, 2008, Phase 1. Vol. 1. Report 2, p. 32). Based on the action plan, there were five vast areas which could help restrict harmful and illegal online content.

- Promoting voluntary self-regulation and content control among the public, using hotlines and asking them to report harmful material
- Providing regulation tools and rating systems which activate parental and teacher control over internet content available to children
- Improving awareness among users about such provisions, thus helping them increase their influence
- Dissecting the legal concepts and definitions of a safer use of the internet
- Encouraging international cooperation in internet regulation (Amn Afzar Gostar Sharif Service Provider, 2008, Chapter 1. Vol. 2. Report 2, p. 32; Deibert et al., 2008, p. 187).

In the first category, it is noteworthy that in order to limit a flow of undesirable, harmful, and illegal content the establishment of a self-regulating order is an essential element. After the above proposal

established, the relevant committee and panels on self-regulation and co-regulation were set up in 2004 to meet the following objectives:

1. Facilitating the network connection among appropriate structures of the member states and strengthening the bond between self-regulating systems outside Europe
2. Facilitating self-regulation on such matters as a quality rating of web pages
3. Encouraging service providers to draft codes of conduct
4. Promoting research aimed at increasing the effectiveness of rating projects and the regulation technology (Jalali Farahani, 2007, Vol. 2, p. 18-19).

The focus in this area is to activate the public capacity. Alongside the hosting servers and access providers, there is a third entity titled "Hotlines" consisting of professional private institutions. Hotlines play a key role in organizing and purifying the cyberspace and are being backed by the European Union and the national authorities. For example, INHOPE is a collaborative professional body, supported by the EU, which has launched 25 hotlines in 23 countries worldwide. The hotlines are ordered to convey warnings and reports to the service providers, police, and members of the foundation. A similar entity is Britain's Internet Watch Foundation (IWF), which has reported its cooperative approach has helped reduce the country's child abuse rate from 18% in 1997 to 4% in 2004 (Frybman et al., 2008, p. 180-181).

In the second category, emphasis is put on technical provisions, enabling users to limit and manage their exposure to unfavorable and harmful content as well as unwanted spam material. To do so, the following steps have taken:

1. Assessing the efficiency of the available regulation technology
2. Facilitating and coordinating the best plans and the information transfer process
3. Increasing public cooperation regarding content and the quality tags of webpages
4. If necessary, offering cooperation on making available the regulation technology in languages which have not yet been covered.

There are a few points to be mentioned in this regard:

1. Only technical measures which observe privacy protection legislation will be supported.
2. Since the private sector does not invest in developing and producing regulation software, part of the budget plan should be allocated for that purpose.

3. Meanwhile, some budget also needs to be allocated to improving the efficiency and transparency of such tools.
4. The tools are mainly devised for users and are meant to help them consciously select their online content. This part of the project receives around 16 to 23 percent of the entire action plan's budget (Jalali Farahani, 2007, p. 18).

The third area asserts that public awareness of the layers of illegal, unwanted and harmful content needs to be elevated, while also supporting users and data as well as information and network are significant. It also demands that the expanding educational material addressing children should be placed on the agenda, since they are making much greater use of the internet compared to parents. Such plans should be implemented in the most appropriate and least costly manner and transferred through means of communication. Given the high significance and the important role of awareness among children and parents in preventing internet threats and tackling the challenges, this area receives 43 to 50 percent of the action plan's budget (Jalali Farahani, 2007, pp. 19-20).

5. China

When it comes to both the quality and quantity of the internet regulation success, China is probably standing at the top, as a country that has "institutionalized the world's most comprehensive regulatory regime in different network layers covering and blocking a variety of subjects," (Deibert et al., 2008, p. 20). Such a position in internet regulation plus the similarity of China's policy structure with that of Iran and the common strategies used in both countries, make China a significant case for the purpose of this research.

5.1. Policy-Making System

The ruling political and ideological structure in China that is based on communism has defined magnificent and widespread state influence in all sectors of Chinese life. The same holds true for the issue of internet regulation, where the country's policy-making structure is visible and dominant. "Nearly from the introduction of the internet into China, the central government has realized that there were unknown potentials. Therefore, to prevent all the possible consequences, it took over not only the full ownership, but also the entire control over the new phenomenon (Jalali Farahani, 2007, p. 7). Yet, here, state policy-making does not necessarily deny the private sector's role.it serves as the channel through which state power and influence are exercised. For instance, content

control and state censorship are carried out through the supervision of non-state actors including foreign investors. Also in China, every individual is directly responsible for the content of the material they illegally publish on the net. At the same time, users who open up chart rooms or news groups are subject to be controlled and need to be approved by official sources (Frybman et al., 2008, pp. 184-185).

5.2. Legal System

The followings are the policy-making entities in China:

- Ministry of Information Industry: in charge of setting laws, owns telecommunication services
- General Administration of Press and Publication (GAPP): oversees content published by all newspapers, weeklies, monthlies, books as well as webpages
- Ministry of Public Security: drafts the general guidelines and rules applied to internet use
- Central Propaganda Department: makes sure that all published material is authorized and complies with China's communist ideology (Amn Afzar Gostar Sharif Service Provider, 2008, Chapter 1. Vol. 2. Report 2, p. 43).

Since 1996, the Chinese government has issued a large number of rules and directives on regulating the internet. The country's Ministry of Information Industry has implemented extremely restrictive laws aimed at preventing the publication of political interpretations which are not favored by the ruling system. This has led to the repeated issuance of many international reports on the Chinese government's measures, to block various foreign and rights advocacy websites (Fray, 2006 cited by Ameli, 2011, p. 352). Some of those directives and rules have been enumerated below:

- In March 2002, the Chinese government ratified the "the voluntary Public Pledge of Self-Discipline for the China Internet Industry" which demands that the signatories legally oversee all the information which users publish on their pages and immediately remove harmful content. The same plan forbids any connection to all corporations which transfer harmful material. Most internet giants in the United States have approved of the Chinese demand, signed deals with Beijing and agreed to cooperate with the Chinese government's internet content control and message oversight system. China also managed to convince Google to launch the filtered version of its search engine in the country (Frybman et al., 2008, p. 185).

- In 2007, the state Radio and TV Organization alongside the Ministry of Information Industry jointly drafted a series of executive conditions for audio-visual internet services, based on which all online audio and visual severs need to receive work permits from Chinese state authorities (Ameli, 2011, p. 354).

5.3. Technical-Executive System

China's internet regulation system is worth studying as it is equipped with one of the world's most complicated, penetrating and wide-reaching technical and executive structures (Amn Afzar Gostar Sharif Service Provider, 2008, Chapter 1. Vol. 2. Report 2, p. 14). This section explains the role of the concerned institutions and the key players in the field of regulation in full detail.

From the technical point of view, regulation is enforced in all of the three levels of the structure of China's cyberspace. Therefore, this process is applied to the backbone network and is also employed by the service providers, home users, administrative users and the owners of cybercafés (Amn Afzar Gostar Sharif Service Provider, 2008, Chapter 1. Vol. 2. Report 1, pp. 17-19). Below is an explanation of the key players of the internet in China and the part they each take.

Level 1. Backbone network

What has been designed and implemented at this level as a massive national project is called the "Golden Shield" or the "Great Firewall" (Ameli, 2011, p. 353). The project is, in fact, China's most important technical tool in internet access restriction. The firewall explores all the data packs and dynamically detects packs which contain the forbidden keywords, and then disconnects the link (Dibert et al., 2008, p. 37). The infrastructure can also be applied to emails, blogs, online boards and search engines (Hang, 2006, cited by Jalali Farahani, 2007, p. 8). The system has hired an army of thousands of human forces who directly oversee the online activities of users across China. The Chinese government considers such a system an essential factor in helping create a healthy cyber environment for Chinese people (Rouzbahani, 2014, p. 85).

Level 2. Internet service providers

- Access service providers

These servers are all from the private sector and the intermediary between the national connected networks and the final users. They all have to supply their wide band through the backbone network. Access providers are required to record information on every 60 days of the

online activities of the users, including registration numbers, phone numbers, addresses and domains of the pages visited and the connection times and hand over the data to the concerned authorities when they request them (Jalali Farahani, 2007, p. 8).

They are also required to install tracking software, implement oversight and control strategies and report to the relevant authorities once they detect a user with illegal activities. The servers also need to install programs to filter webpages deemed as saboteurs by the government (Frybman et al., 2008, p. 185). In a wide network, the major servers should further regularly share and exchange information about the banned websites. (Hang, 2006, cited by Jalali Farahani, 2007, p. 8).

• Internet Content Providers (ICPs)

The ICPs are concerned with issuing permit requests for businesses and in non-commercial areas they are responsible for releasing and filling in the special forms. They are required to control the content of their pages and immediately respond to any illegal material (Amn Afzar Gostar Sharif Service Provider, 2008, Chapter 1. Vol. 1. Report 2, p. 20). Therefore, according to Chinese law, all content providers need to register their identity with the central or provincial offices of the Culture Ministry (Amn Afzar Gostar Sharif Service Provider, 2008, Chapter 1. Vol. 2. Report 2, p. 37).

When it comes to news and media websites, Chinese control gets even tougher. Indeed, news story publishing on the web is in general forbidden unless it is done through a web page belonging to a government office or the State News Center Institutions. If a specific internet portal seeks to publish such news stories it has to observe all the specified conditions regarding professional editorial guidelines as well as financial resources and technical provisions (Amn Afzar Gostar Sharif Service Provider, 2008, Chapter 1. Vol. 2. Report 2, p. 37).

The same holds true for public websites. They are required to install the security software which can review and record all the messages sent and received by the users and report to the government all the "sensitive cases" (E.F.E. 2002, cited by Ameli, 2011, pp. 353-354).

One clear example here is the agreement between the Chinese government and Google. China has recently been using a new filtering method, based on which Google has agreed to refrain from opening specified page results for the search attempts by Chinese users (Diber et al., 2008, p. 48; Rouzbahani, 2014, p. 85).

In addition to such preventive measures, the Chinese government itself has further placed large emphasis on internet search services. To

do so, it has established and expanded two home-grown and domestic engines, dubbed "Baidu" and "Yaesu". While users search the sensitive keywords, the two engines will immediately prevent access and block the pages (Hang, 2006, cited by Jalali Farahani, 2007, p. 8).

Level 3. Final users

• Cybercafés

Since personal computers and home internet connection are not affordable by many people in China, cybercafés have found a special place where government control is heavily concentrated. The Ministry of Information Industry, the Culture Ministry, the Ministry of National Security and the Trade and Industry Department are responsible for regulating China's cybercafés (Hang, 2006, cited by Jalali Farahani, 2007, p. 9).

Opening up a cybercafé in China is quite a demanding and complicated paper work process. In addition to going through such a stage, the owners must provide authorities with all the information regarding their working structure, the number of computers, the domains as well as their IP addresses, while also installing oversight software. In 2001 alone, 17,488 cybercafés were shut down. 28,000 others also received orders to immediately install the necessary oversight software. Alongside those control mechanisms, there are also cyber officers known as "Wang Guans" who constantly monitor the content and the users' activities (Amn Afzar Gostar Sharif Service Provider, 2008, Chapter 1. Vol. 1. Report 2, pp. 18-19; Amn Afzar Gostar Sharif Service Provider, 2008, Chapter 1. Vol. 1. Report 1, p. 20; Hang, 2006, cited by Jalali Farahani, 2007, pp. 9-10).

• Final user

Chinese users are required to register their personal computers to help accelerate the process of identification and surveillance conducted by the state. All users must sign a statement of obligation in which they express commitment not to jeopardize national security and public safety. The same approach applies to service providers. They are responsible for the activities of their clients, something which has pushed them toward extreme filtering methods (Hang, 2006, cited by Jalali Farahani, 2007, p. 10).

Conclusion

By this point, the paper has briefly reviewed three regulation systems rooted in three different approaches. The study of those systems

exposes one to a series of ideas and proposals which could be applied to improve Iran's regulatory system. In the conclusion section of this chapter, a comparative analysis of the three systems is offered, in which the differences existing among them are highlighted and the extracted finalized policies proposed for the Iranian system are fully elucidated.

- Comparative analysis

Different criteria exist, using which one can make comparisons among various countries. The paper has sought to draw the analogy among the three case studies based on factors such as policymaking, ownership, management, physical status, and time and software production quality.

Perhaps the most important criterion that distinguishes regulation systems could be sought in the policy-making structure. Earlier, the three strategies in policy-making including state regulation, co-regulation and self-regulation were fully discussed, where the research found out that the US is a country in which the third approach is employed. Although the legal cases of exception were alluded to, in which the state interferes, those cases were limited and the general regulation was conducted by the private sector. Proof for that is the large number of private regulation software developing firms, a multitude of private companies involved, regulation carried out through parental control, at schools, libraries, by service providers, etc. Here, the Digital Millennium Copyright Act (DMCA) is worthy of reference as a case in which the protection of such a right has been agreed upon by intellectual property owners and representatives from electronic businesses. The European Union, on the other hand, is where the co-regulation system is enforced and the cooperation between states and the private sector is emphasized. One evident case of such a strategy is the "hotline" project which is meant to create some infrastructure whereby state monitoring is done through the public's eyes. The same level of cooperation is also visible in the three-year programs. The case of China, however, is an example of strict state regulation, in which the "Great Firewall" serves as the most significant project in a mere-government control of the cyberspace.

The status of different countries in other criteria could be predicted based on their regulatory systems. The second criterion is the ownership structure. Given the special importance attached to the private firms in the United States, the ownership system, there is non-monopolist, while in the EU it is semi-monopolist (proof of which is the "hotline" project and the private software producers). In China the case is one of full

monopoly, as it is the state which is in complete control of developing the regulatory software.

When it comes to the management order, the issue is different. In the US, it seems that the six-point laws allow for a more palpable presence of the ruling system in regulation. One example is the federal government's influence over regulation in libraries and state-run schools or the measures which have been devised to tackle child pornography. Thus the US management system in regulation has to be considered as a semi-centralized one. The same system, in a more serious fashion, is common in the European Union, while in the Chinese version it is entirely centralized. This is proven by the law which obliges everyone to register their computers in a centralized state-controlled database.

Another criterion for comparison could be the issue of "physical status" of the regulation system. As mentioned earlier, such a status has three aspects: 1-the communicated, 2-the channel, 3-the communicator. It seems that in the US, although the regulation process is focused on the communicator, it is partially applicable to the channel and the communicated as well. The key current of regulation in the US is dedicated to the production of home regulation software. Schools and libraries also install them, while access providers also play a major role in controlling child pornography, especially when such services are demanded by the users.

What is emphasized in the US, particularly when it is concerned with the fields of security and copyright, the priority is given to content removal rather than blocking. This is practicable given the fact that the US is home to the world's major hosting infrastructure. Likewise, in the EU the regulation system exists in all the three fields, where the key role is played by the final users and the communicated themselves. Still, the part taken by access and hosting service providers in the EU is stronger than in the US. In China, serious concentration is placed on all the three. But the state role in the channel field with the firewall system is much more serious. Still, in China, content and access providers as well as cybercafés are required to install regulation software on their systems.

The criterion of time is the same in all the case studies, where it is of a perpetual nature. In other words, regulation is constant in all of them and does not have time limits. For instance, it does not temporarily stop during election times. In such cases, it even gets tougher and stricter. Finally, one can also allude to the quality of the production of the software. In all the cases, the US, the EU and China, it is domestic and homemade.

Table 1 offers in a nutshell the results of the comparison among the three cases.

Table 1. A comparative analysis of the subject countries

Country Criteria	US	EU	China
Regulation system	Self-regulation	Co-regulation	State-regulation
Ownership order	Non-monopolist	Semi-monopolist	Monopolized
Management system	Semi-centralized	Semi-centralized	Centralized
Physical status	Communicator, channel, communicatee	Communicator, channel, communicatee	Communicator, channel, communicatee
Time	Perpetual	Perpetual	Perpetual
Software production fashion	Homegrown	Homegrown	Homegrown

- **Policy proposals for the case of Iran**

The following section firstly reviews the measures employed by the countries which are the subjects of the research. A package of proposals will be presented afterwards.

• **Key measures**

1. Investing and concentrating on the final user

The striking point one comes across while studying the cases of the US and the EU is their focus on the final users. The experience in those two locations has proven that the shift from the national and macroscopic regulation system to microscopic and individual ones is more workable and efficient. Such a concentration has the following characteristics:

1.1. Special attention attached to children and young adults. As a general rule, the Western world places high significance on children and young adults as vulnerable communities. Therefore, important measures are developed to protect their health and safety in the cyberspace. Examples are the age rating for content, age verification processes, criminalization of child pornography, promotion of cyberspace literacy and knowledge, etc.

1.2. Parental role. For the same reason mentioned above, parental role is of high seriousness in both the US and the EU, where governments have been trying to prepare the ground for the control and oversight of parents on children's use of the internet. For such a purpose, a variety of software versions are exclusively developed and parents receive training and educational awareness.

1.3. Empowering the users (social prevention) and improving media literacy. In general, the issue of social prevention through training and awareness raising and thus empowering the users is a serious policy both in the US and the EU. In fact, it seems that the two have found out that it works as a fundamental and effective solution for purifying the cyberspace if users voluntarily protect themselves from being exposed to harmful, offensive and inappropriate material.

1.4. Making use of public capacity in surveillance. One of the basic policies adopted by the European Union, which has proven quite successful, is taking advantage of public capacity in detecting offensive content. To do so, the major practical step taken has been launching "hotlines", which has been warmly welcomed by the users and can be adopted in the case of the Islamic Republic of Iran.

2. Using economic strategies

2.1. Enforcing cooperation with state institutions. Based on the CIPA (Children's Internet Protection Act), US schools and libraries which receive federal funding are required to install regulatory software if they are willing to continue to receive the financial support. This means that "economic leverage" can be taken advantage of as a tool to improve the effectiveness of the regulation system. The policy can be particularly workable when applied to public surveillance, private sector investment, etc. It is also worthy of note that such economic measures can be punished and have a preventive nature while also serving as incentives.

2.2. Creating competitive market. The research found that in the case of the US, there is a serious market competition among companies producing regulation software, an atmosphere which can improve quality and balance the prices.

3. Special attention to state and public institutions

In almost all the cases studied here state and public institutions are treated as significant entities in regulation. Basically, the economic logic in government offices is that the general use of the internet by employees

remains controlled and overseen. In the US, this is more striking in the case of schools and libraries. In China, also there is a complicated surveillance system controlling user activities in cybercafés.

4. Prioritizing content removal over blocking (special role played by hosting service providers)

Based on a technical logic the removal of content is preferable over blocking, as it totally destroys the chance of circumventing the regulation measures. This is where the role played by hosting service providers becomes more effective and visible. Still, the technical prerequisite for such a policy is the fact that the hosting infrastructure has to be homegrown and data centers, which could offer an efficient contribution to content servers and service providers, must exist.

5. Agreements with foreign companies

This is an issue which China has especially paid attention to by signing deals with such internet giants as Google and Yahoo. Negotiating with major service providers, search engines, email companies and social networking websites not only prepares the ground for new services in the host country, it also expands the surveillance and control strategies which the host governments can hire. In fact, transferring the data centers of those companies to the host country brings positive results for both sides.

6. Content rating system

The system has been actively implemented in the US and the EU, where officials have come to the conclusion that the policy is essential in making the society user- oriented and showing respect to the decisions taken by the users, particularly children and young adults. In such a system age rating is a priority. There are also others ideas applicable to occupational, educational, gender, ethnic and cultural ratings.

7. Using international cooperation capacities

Finally, another plan pursued with great attention by the European Union has been set up international institutions dedicated to purifying the cyberspace with regard to common concerns shared by world nations. It seems that in the case of the Islamic Republic of Iran attention to international areas, particularly a regional focus on the Islamic world must be placed on the agenda.

- **Alternative proposed policies**

1. Decentralization policy

The experience in the United States and the European Union proves that cyberspace regulation demands a comprehensive plan and

that measures should not be specified to state and central levels. In other words, in such areas as policymaking, structures, human resources and processes, steps have to be taken to shift the focus toward decentralization. Such a policy in the first stage of regulation suggests a need for co-regulation and then self-regulation. With regard to structures and human resources, the same strategy proposes decentralized management and the active presence of different players in the cyberspace. At the operational level, it also calls for using various processes from cultural, economic, political, legal and technical fields. In what follows more light has been shed on the different aspects of the policy:

1.1. Co-regulation and private policymaking. With regard to the ratification and the oversight of the implementation of the legal aspects of regulation, state policymaking is exclusively centralized, in which the government and the ruling system is the only decision maker. However, in a progressive system, joint regulation is followed, in which both the state and the private sector share efforts in creating the order. This basically reduces the centralized nature of regulation. In even more advanced levels, regulation is totally handed over to the private sector, with a massive diversity of players who make the system a wide-reaching one, spread across the board, which is by nature a positive structure.

1.2. Structure and human resources-decentralized structure. Based on the policy principle mentioned, all the state institutions and structures as well as individual players must take part in the regulation process, as it should not be limited to governmental and national levels. Then the following would be the key players from the intuitional and individual levels:

- **Users.** At the user level, priority is given to raising the media literacy and strengthening the self-control skills. Meanwhile, the role of oversight played by parents and teachers over children's internet behavior as well as the expansion of employers' surveillance over staff members in offices and a focus on regulating online activities in cybercafés are of significant value.
- **Hosting servers.** Hosting service providers are among the major players in the field of regulations. The significance of investing in them lies in the fact that they are associated with less non-material costs and could be capable of improving the quality of regulation by destroying the possibility of

circumvention. Still, the most important necessity here is the popularity among users and the quality of hosting services offered to both domestic and foreign clients.

- **Access providers**. They are playing an important role in different countries and it seems that more attention needs to be paid to them, especially when they are asked to offer regulation products as their value added services.
- **Domain Name providers**. They have remained largely ignored, while they have great capacities in reducing the possibility of circumvention to a zero level.
- **Content & service providers**. Since they are of an important share in the virtual world, they need to be given more space in the regulation process. Ideas to be considered in this regard are disseminating the culture of social responsibility, negotiating with foreign firms, establishing homemade search engines and setting up registration or declaration systems in the business field.

1.3. User-oriented policy. The role of users in the Iranian cyberspace is not just limited, it is ignored indeed, despite the fact that they are the very major players in the field and that there must be growing attention shifted toward them. The following are proposals in this regard:

- Attention to vulnerable users: There is a need to develop special regulation orders for the society's vulnerable communities, children and young adults in particular. For instance, regulation based on the white list is a measure adopted as a successful experience in some countries.
- Parental role: Another example of orientation toward users is oversight over children, as a role played by parents. At any rate, raising children is the natural duty parents in the first place. The same holds true when they enter the cyberspace as well. Therefore, there is a need to place on the agenda plans for raising parental awareness and providing them with oversight programs.
- Attending user needs: Another quality of a user-oriented policy is that it should set up the regulation based on the needs and the abilities of the users. In fact, since user demands differ, one single regulation system might prove incompetent. The best proposal in this regard seems to be a multi-level regulation system or one based on age ratings, taking into account special demands of each group.

- Offering regulation services based on user requests: One helpful idea is the content providers' efforts to offer added value services in the regulation field. Those services are based on requests from users who pay for them in return.
- Empowering the users: Attention to the value of users can be demonstrated in the form of efforts to improve their media literacy. It is worth noting that one of the most fundamental, original and sustainable solutions used to purify the cyberspace are offering those educational points and awareness so that they will independently decide to live a healthy life on the internet.
- Surveillance through the public: Given the flowing and dynamic nature of message distribution in the cyberspace, centralized surveillance systems fall short and would prove under-staffed in terms of human resources. One useful idea to handle the issue, therefore, could be activating the public regulation capacity.

1.4. "Preferring removing to blocking" policy

The experience in such countries as the United States, where lies most of the world's internet infrastructure, especially in the hosting field, has proven that for regulation at a national level removal of content is preferred over blocking. The two techniques differ in the following:

- In removal both the message and the content are uprooted from the network. Then the possibility of circumvention wouldn't make sense anymore. Thus, naturally search engines would also fail to revive such material. However, in blocking both the message and the content still exist in the network and it is only the access which is denied.
- Removal is done by hosting servers, while blocking is carried out by access providers.
- The negative cultural and psychological consequences of removal are much less significant compared to blocking. In addition, when content is removed the friction only develops between the user and the content producers or the hosting servers and there is no tension with the regulator. But when material is blocked both tensions will grow between the users and the regulation system. The policy of content removal and the preference over blocking applies to cases in which communication infrastructure, especially hosting servers are controlled by the state. Therefore, a highly useful approach

and a feasible one to be taken into account and employed at Iran's newly-developed "National Information Network".

1.5. "Preferring surveillance to filtering" policy

Investing on surveillance in cyberspace could be regarded as a tool showing the ruling system's authority. It seems that a state by enforcing maximal filtering while there is the possibility of using proxies will only will be reducing its own power and turning the internet into a tool against its own security and authority. It is therefore, highly recommended that the internet's surveillance capacity in analyzing the response and behavior exhibited by users in the face of filtering is applied to wider and more appropriate policymaking. Prioritizing surveillance over filtering firstly helps with improving individual users' self-oversight and secondly prepares the ground for the ruling system to strengthen its authority in the virtual world. To gain such an objective, the two following are proposed:

- Content rating and sorting: It refers to controlling the content in the virtual world and rating and classifying it, thus giving the users the option to choose the material conforming to their taste and demands. The measure could be particularly useful in protecting children and young adults and keeping them immune in the face of harmful material.
- Monitoring and analyzing user behavior: Closely following the behavior demonstrated by users is one first step toward assessing their responses and thus devising policies accordingly. This paper attaches great emphasis to a cultural and communicational observation and analysis of user behavior and applying it while relevant policies are drafted and decided upon.

Note

This paper has been adopted from the doctoral thesis written by the second author and supervised by the first author at Imam Sadiq University.

References

Ameli, S.R. (2011). *Rooykarde dofazaei be asibha, jarayem, ghavanin va siasathaye fazaye majazi* [dual-spacization approach toward harms, offences, laws and policies of Iran's cyberspace]. Tehran: Amirkabir Publications.

Amn Afzar Gostar Sharif Service Provider (2008a). [Comparative studies in other countries' approach toward internet regulation] (Phase

1, Vol. 1, Report 2). Tehran: Iran Telecommunications Research Center.

Amn Afzar Gostar Sharif Service Provider (2008b). [Legal status and challenges regulating the internet in national and international levels] (Phase 1, Vol. 2, Report 2). Tehran: Iran Telecommunications Research Center.

Ansari, B. (2011). *Hoghoghe ertebate jamei* [Mass Communications Law]. Tehran: Samt Publication.

Balkin, J.M., Noveck, B.S., & Roosevelt, K. (1999). *Filtering the internet: A best practices model*. The Information Society Project at Yale Law School.

Child Online Protection Act (COPA) (H.R.3783). (1998). Retrieved from Library of Congress website: https://www.congress.gov/bill/105th-congress/house-bill/3783.

Children's Internet Protection Act (CIPA). (2000). Retrieved from https://www.fcc.gov/consumers/guides/childrens-internet-protection-act.

Costello, R.B. (1992). *Random House Webster's college dictionary*. New York, NY: Random House.

Deibert, R., Palfrey, J., Rohozinski, R., Zittrain, J., & Stein, J.G. (2008). *Access denied: The practice and policy of global internet filtering.* Mit Press.

Digital Millennium Copyright Act (DMCA). (1998). Retrieved from https://www.copyright.gov/legislation/dmca.pdf

Electronic Commerce Directive. (2000). Retrieved from http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32000L0031

Frybman, B., Hennebel, L., & Lewkowicz, G. (2008). Rahbordhay dolati baray samandehi moshtarake internet dar Amrika, Oroopa va Chin. [Public Strategies for Internet Co-regulation in the United States, Europe and China]. (M. A. Nouri, Trans.). *Law Information Journal*, *6*(14), pp. 171-188.

Illegal and harmful content on the Internet. (1996). Retrieved from http://aei.pitt.edu/5895/1/5895.pdf

Jalali Farahani, A.H. (2007). [*Taamoli bar filtering (motaleye tatbighi sayer keshvarha).* A Review of Filtering (A comparative study on other countries)] (8442 Vol. 2). Tehran: Iran Parliament Research Center. "Studies on Communications and New Technologies". Retrieved from http://rc.majlis.ir/fa/report/show/734106.

Rouzbahani, M.R. (2014). *Jaygahe feghhi va hoghooghie filtering (mahdoodiat) dar rasanehaye majazi az didgahe mazahebe khamse* [Filtering in Virtual Media from Legal and Jurisprudence Perspectives]. Tehran: Ketab Ava.

Summers, D. (2003). *Longman dictionary of contemporary English*. Essex: Pearson.

USA Patriot Act. (2001). Retrieved from https://www.justice.gov/archive/ll/highlights.htm.

Wehmeier, S. (Ed.). (2005). *Oxford Advanced Learner's Dictionary of Current English*: AS Hornby. Oxford University.

The voluntary Public Pledge of Self-Discipline for the China Internet Industry. *Communications Decency Act (CDA)*. (1996). Retrieved from https://internetlaw.uslegal.com/free-speech/the-communications-decency-act-of-1996/.