THE GUARDED OPENNESS: THE CHINESE WAY TO GOVERN THE INTERNET

Elisa Bertolini

Professor in Bocconi University, Milão.

TABLE OF CONTENTS

I INTRODUCTION

The article provides for an outline of internet governance in China and the protection of fundamental rights, in particular freedom of expression.

The issue of the internet governance is one of the major debated by scholars in recent years and the solution seems very difficult to reach. Indeed, the problem is not only the issuing of a comprehensive regulation of the net, since such regulation has also to protect the fundamental rights of the individual.

If we examine the technical structure of the internet, we can say that it is a completely different media in comparison with the traditional ones, such as newspapers, radio or TV broadcasting. But that does not mean that it is impossible to establish a legal framework that regulates it. A regulation is essential because the plurality of subjects – ISPs, ICPs and users – using the internet to provide services and contents, to communicate, to look for information or to express their opinion, need their rights to be legally protected. However, cyberspace presents something new for those who think about regulation and freedom. It demands a new understanding of how regulation works. Changes in technology almost inevitably destabilize the existing regulatory environment.

How to regulate cyberspace? Is it inherently not regulable by territorially based sovereignty, and should be seen as its own legal jurisdiction (multiple-jurisdiction) as Post says?[1] Or is internet only a medium through which people in real space in one jurisdiction communicate with people in real space in another jurisdiction, being more complex than the real space, thus regulable by national regulations as Goldsmith contends?[2]

Internet, cutting across international borders, undermines the legitimacy of law based on geographic boundaries. Cyberspace has no territoriality based boundaries and it can create its own law and legal institutions. Nevertheless, a set of legal rules is necessary. Cyberspace has destroyed the relationship between a phenomena and its physical location, weakened the power of local government to assert control over on line behavior. But this does not mean that a sovereign State can not legitimately determine an internet governance or international organizations a global one; at the same time, beside national regulations, a self-regulation of cyberspace can take place.

Claiming the impossibility to issue such a governance means to leave the anarchy rule the net, originating situations in which the fundamental rights and freedoms of

[1] David R. Johnson & David G. Post, Law and Borders–The Rise of Law in Cyberspace, 48 Stan. L. Rev. 1367 (1996). David G. Post, Against "Against Cyberanarchy", 17 Berkeley Tech. L.J. 1365 (2002).
[2] Jack L. Goldsmith, The Internet and the Abiding Significance of Territorial Sovereignity, 5 Ind. J. Global Legal Stud. 475 (1998): Idem, Against Cyberanarchy, 65 U. Chi. L. Rev. 1199 (1998).

the individual are infringed. Its particular features, above all the trans-nationality, the fluidity and the continuous technological development, surely make it more difficult to issue a global and efficient regulation, but not impossible. Moreover, considering its multi-jurisdictionality, also the legal framework, the governance of the internet, should be global and based on the consensus of the majority of the international community. Therefore, the target should be the issuing of global, detailed and organic governance that offers protection to the rights and freedoms of the individual. Then the question is how to reach such consensual governance.

Analyzing the Chinese case, it comes out that the Chinese government has set up a comprehensive regulation of the internet, controlling every key point of the net. The behavior of every cyber-actor is strictly regulated, and this in a very efficient way. The problem is that this kind of governance reflects the intents of an authoritarian regime, therefore no legal protection is guaranteed to the freedom of expression, the right to privacy and to access to information. The main part of the article is devoted to how the Chinese Government censors the freedom of expression and infringes the privacy of net surfers.

The examination of the Chinese framework demonstrates that is possible to issue a regulation of the internet, despite, the fact that due to its limitation of freedom of expression, it is not suitable to become the model of global governance. Indeed, the statement of possible governance does not completely solve the problem, since other questions are still open: first, what subject should be entitled to determine the governance and second, which are the best instruments to achieve it? In the final part, the article tries to answer these questions, providing possible solutions.

II CONSTITUTIONAL OUTLINE OF THE PROTECTION OF RIGHTS

Before analyzing the *corpus* of the internet regulations and its influence on the freedom of expression, it is convenient to consider the constitutional framework, so as to check whether there is a mismatch between the constitutional guarantees and the internet regulations.

The Chinese State, as stated in the present Constitution, last amended in 2004, respects and preserves human rights (art. 33, par. 3) – thus overcoming the traditional socialist belief that rights are a bourgeois ideology – the freedom of expression (art. 35 and 41) and the secrecy of correspondence (art. 40). The protection of the right to privacy descends form a broad interpretation of art. 38, guaranteeing the human dignity. The bill of rights until art. 50 does not differ from the ones of Western Constitutions, but art. 51 greatly limits the enjoyment of the rights previously guaranteed. Indeed, art. 51 states that: «The exercise by citizens of the People's Republic of China of their freedoms and rights may not infringe upon the interests of the State, of society, and of the collective, or upon the lawful freedoms and rights of other citizens». Another important limit is expressed by art. 53: «Citizens of the People's Republic of China must abide by the Constitution and the law, keep State secrets, protect public property, and observe labor discipline and public order and respect social ethics». Their disclosure is also punished by art. 111 of the penal code. Art. 53 introduces a fundamental issue that in the internet regulations is used as the main limit to the freedom of expression: State secrets. The 1988 State Secrets Law defines State secrets as «all issues relating to the security and interests of the nation, determined in accordance with legally defined procedures, the knowledge of which is restricted to a defined scope of personnel for a defined length of time». The 1990 Measures for the Implementation of the Law on the Protection of State Secrets, at art. 4, list in eight points the matters that, if disclosed, can endanger State security: «(i) jeopardizes the ability of the national government to maintain stability and defend itself; (ii) affects the integrity of the nation's unity, solidarity among peoples or social stability; (iii) harms political or economic interests of the nation with respect to the outside world;(iv) affects the safety of any national leader or foreign dignitary; (v) hinders important national safety or health work; (vi) causes a reduction in the effectiveness or reliability of any measures to protect state secrets; (vii) weakens the nation's economy or technological strength; (viii) causes any national organ to lose its ability to exercise its legal authority». Other provisions on the issue are in the 1993 State Secrets Law and in the 1994 Measures for the Implementation, but they do not renew the ones of previous regulations. Despite the number of provisions and regulations on State secrets, the meaning of this expression is not clear and is still undefined; there are no objective criteria to decide whether a matter should be considered a State secret of not. Therefore, the authorities can broadly interpret the definition, limiting at the most the freedom of expression of the individual.

Analyzing constitutional and regulatory provisions, a mismatch emerges. The regulations are contrary to the supreme law of the country. But how can this be possible? Basically, we can say that in the Chinese legal system there is no enforceable norm against which the regulations, including the internet ones, can be measured. Therefore, although the Constitution protects the right to freely express and the right to privacy, it is itself not directly enforceable, allowing regulations that expressly violate these rights to escape any form of judicial review. Furthermore, the Constitution, despite the provision of a Constitutional Court, does not provide for a constitutional organ titled to carry out a judicial review. This means that the Chinese legal system does not provide for any judicial instrument to really protect the rights constitutionally guaranteed.

III THE MEDIA SYSTEM AND THE PROTECTION OF FREEDOM OF EXPRESSION

After considering the constitutional background and before considering the internet, let us briefly examine the media regulations, as a background to the internet ones.

We need to say that all the sub-constitutional regulations shall apply only to the Chinese territory, therefore not to the two special administrative regions of Hong Kong and Macao, both characterized by their own legal system.

As previously said, the Constitution guarantees freedoms and rights that are the basis of the existence of a media system, however, the exercise of these freedoms is subordinated to greater values such as the unity of the nation, the security of the State and the social order.

All the regulations concerning publishing, newspapers, satellite, radio and TV broadcasting protect the freedom of expression, but at the same time they provide for broad limitations from both in terms of content and access. Both these forms of limitation act like censorship, but the first is a direct one, because it affects the contents, whereas the second one is indirect, being a control of who enters the system

Concerning contents, each operator must obey the directives issued by the Party and the Propaganda Department and can not deal with matters considered harmful to the security of the State and the social stability. In this direction, the 2002 Notice Regarding the Further Strengthening of the Administration of Selection of Articles for Newspapers and Periodicals states that contents «must firmly grasp the path of the political consensus, strictly obey the press and publication administrative rules and the Party's propaganda discipline, and adhere to political awareness in manuscript contents. They shall not submit or transmit drafts that are contrary to the guidelines of the Party or the nation»; similarly, the 2000 Notice Regarding Further Strengthening the Administration of Periodicals Relating to Current Affairs and Politics, General Lifestyle, Information Tabloids and Scientific Theory, that states that periodicals «must uphold the correct political direction».

Specifically on harmful information, the 2001 Notice Regarding Prohibiting the Transmission of Harmful Information and Further Regulating Publishing Order: «No one may establish an entity whose primary purpose is to transmit news information and engage in other news publishing activities without permission from the press and publication administration agency». Again, the need to protect State secrets, whose relationship with the information is considered in the 1992 Regulations on the Protection of Secrets in News Publishing, affirming at art. 15 «Anyone wishing to provide a foreign news publishing organization a report or publication with contents that relate to the nation's government, economy, diplomacy, technology or military shall first apply to their unit or their supervising organ or unit for examination and approval».

Considering the access, the regulations provide for a license system. Therefore, each operator that wants to enter the communication and information market must obtain a license from the Minister of Information Industry. The license system is a barrier that constitutes a prior restraint to the exercise of the freedom of expression. And if it is essential for radio and TV analogue broadcasting, due to the lack of frequencies, it is not for printed materials. A license is required for all printing enterprise, as stated by art. 7 of the 2001 Regulations on the Administration of Printing Enterprises and for the transmission of TV dramas (the 2000 Regulations on the Administration of Television Dramas). Beside the license, other specific requirements are asked: some concern the capital that who wants to enter this market must dispose of, other, more general, are similar to the contents' limitation.

A plurality of institutional actors is entitled to supervise and control the telecommunication field. Besides the Party and the Propaganda Department, the governmental agency GAPP (General Administration of Press and Publication), the Ministries of Information Industry (MII) and Public Security (MPS), the State Council Information Office, the SSB (State Secrets Bureau) and the PSB (Public Security Bureau). They can all issue regulations and implementing measures, therefore these are not organic and badly drafted.

The control exercised by the authorities is not the only one applied to the telecommunication system. Indeed, there is also a more informal control which comes from the inside, from the editors that, through the so called *neican* (internal directives), establish which topics can be dealt with.

The elaborate governance of the telecommunication system reflects the will of the Party to tightly control the topics of discussion in books, periodicals, newspapers, radio and TV, in order to remove any attempt to subvert the regime. Due to its effectiveness, the authorities tried to repeat this model to the internet, with some changes, according to the particular technical features that distinguish the net from the other media.

IV THE INTERNET GOVERNANCE

The internet regulations are very strict and limit at the most the freedom of expression and the right to privacy, despite being rights constitutionally guaranteed. They are a sort of replica of the regulatory model of the telecommunication system, obviously *mutatis mutandis*, due to the particular features of the net. Indeed, the first internet regulations followed the publishing and the broadcasting ones, but afterwards they became peculiar, maintaining however the idea of direct and indirect censorship.

The internet is a medium that amplifies the freedom of expression because everyone accessing the net can express his opinion through BBS, forums or chat-lines, and can also have access to any kind of information. Therefore, the Party fears that the internet may turn into a threat against the regime. The Party's approach to the regulation of the internet can be summarized in the slogan "guarded openness", that conciliates the economic advantages, coming from the openness to the global communications' market with the control aimed at preventing the net to become an anti-regime propaganda instrument.

The first internet connection took place in China in 1987 between the ICA of Beijing and the University of Karlsruhe in Germany. The net officially arrived in 1994 and the commercialization begun the year after. Currently, about 200 million Chinese are estimated to surf the net.

The Chinese internet governance begins in 1994, with the PRC Regulations for the Safety Protection of Computer Information Systems, assigning to the MPS a general responsibility to watch over the net.

However, the first regulation is the 1996 State Council Order n. 195, Interim Regulations on International Interconnection of Computer Information Networks in the PRC. It organizes the structure, dividing the interconnecting networks (INs), which are nine, from the access networks (ANs) – or ISPs – the firsts directly connected to a foreign internet backbone and the seconds retail sellers of internet access purchased from the nine INs. Both INs and ISPs must obtain a license from MII, as provided for the other media.

The Chinese net is organized around the nine INs, who have a ministerial license and are controlled by the great national firewall; the most important are CSTNet (The China Science and Technology Network), ChinaNet, CERNet (China Education and Research Network) and CHINAGBN (China Golden Bridge Network). Therefore, the access to the world wide web is allowed only through them, making the Chinese net a kind of big national intranet. The consumer who wants an internet access must use the connection offered by local service providers that buy it from one of the nine INs. The major infotainments web portals are Sina.com, Shou.com e 163.com, whereas the leading search engine is Baidu.com.

The following regulations are focused on the contents and on ISPs and ICPs that bear the responsibility for the behavior of their customers and for the contents published in their web sites. Regarding contents, they have to censor all information that may be harmful to the national security. The first list of these contents is quoted in the 1997 MPS Measures on the Administration of Safeguarding the Safety of Internationally Networked Computer Information Networks.

Other restrictions on contents and major responsibilities for ISPs and ICPs are introduced by the 1997 Computer Information Network and Internet Security, Protection and Management Regulations. Concerning contents, art. 4 forbids the consumer to use the net in order to threaten the security of the State. Art. 5 lists all the matters that can not be disclosed: inciting to resist or breaking the Constitution or laws or the implementation of administrative regulations; inciting to overthrow the government or the socialist system; inciting division of the country, harming national unification; inciting hatred or discrimination among nationalities or harming the unity of the nationalities; making falsehoods or distorting the truth, spreading rumors, destroying the order of society; promoting feudal superstitions, sexually suggestive material, gambling, violence, murder; terrorism or inciting others to criminal activity; openly insulting other people or distorting the truth to slander people; injuring the reputation of state organs; other activities against the Constitution, laws or administrative regulations. Art. 7 protects the freedom and the privacy of net surfers. Art. 8 establishes that ISPs have to cooperate with the SSB and PBS and to comply with their requests of costumers' private data. ISPs are obliged to store their costumers' data for at least 60 days.

Again on the same issue, the most important regulations are those of the year 2000, dealing with the State secrets, whose disclosure is forbidden also for internet users. The 2000 State Secrets Protection Regulations for Computer Information Systems on the Internet qualify the disclosure of State secrets as a cyber-crime and the 2001 amendment to the 2000 Decision of the NPC Standing Committee on Safeguarding Internet Safety has introduced death penalty for the guilty people. Harmful information for national and social security are also forbid by art. 9 of the MII Provisions on the Administration of Internet Electronic Bulletin Services; art. 10 of the same Provisions affirms that BBS providers who find forbidden information on their BBS have to immediately erase them. This idea is also stated by art. 8 of the Provisions on the Administration of the Protection of Secrets on Internationally Networked Computer Information Systems, that expresses the principle according to which «those who go online shall bear responsibility». In the same direction, the authorities' request to text messaging providers to install filters to monitor and erase dangerous messages.

A healthy development of the internet is the target of the Measures for Managing Internet Information Services, target that can be achieved through a strict control on the internet information services, IISs (or ICPs). They have to watch over the contents published in their sites, censoring and erasing, if necessary, dangerous information. Therefore, each provider bears a direct and objective responsibility. Art. 4 distinguishes the IISs in commercial, that must get a ministerial license, and non-commercial, that have only to register their activity at the official records. Again is repeated the list of harmful information and the need for the providers to store the customers' private data.

The 2002 MII and GAPP's Interim Provisions on the Administration of Internet Publication aim «to safeguard the legitimate rights and interests of Internet publishing agencies and to promote the healthy and orderly development of the Internet publication undertakings of China». Art. 6 is very important because, according to the provisions on ISPs and ICPs, introduces a preventive authorization for all the operators who want to start a publishing activity on the net. The same kind of authorization is requested for the news web sites, as affirmed by art. 5 of the 2000 Interim Provisions on the Administration of Internet Web sites Engaged in News Posting Operations; instead, this authorization is not required for general web sites, that can published information already publish in news web sites.

In order to watch over the cyber-surfers and the opinions they express more efficiently, the Government issued a regulation aiming to ban anonymous posting and establishing the commitment for bloggers to register their blogs with their real names and not with the nicknames usually used in the net. On this matter, the city of Xiamen issued, in July 2007, a regulation that imposes to all the surfers to sign their posts in all the web sites recorded in the city with their real names.

The regulations we have considered until now are national, but besides them there are a lot of regional, provincial and local regulations, outlines and policy documents.

The legal framework of the Chinese internet is highly regulated in every aspect. The behavior of every subject who plays a role in the net is regulated: ISPs, ICPs, customers, the ones who have a publishing activity or who want to broadcast audio-visual programs. Such a comprehensive regulation for the operators does not correspond to a system of guarantees to the internet users, whose fundamental rights, freedom of expression and privacy, are not protected at all. Indeed, the nine categories of harmful information are quite flexible and they can comprehend many other kinds of information that are not expressly mentioned. The main example is the expression ‘State secrets’. This voluntary vagueness allows the public authorities to limit at the most the opponents to the regime. Furthermore, concerning the black holes, we have to say that no regulation is issued in the field of protection of copyright and of illegal download; this lack is due to the wiliness of the authorities, who prefer to concentrate their regulatory efforts in repressing the dissent rather then in protecting rights.

In any case, China has showed that internet governance is really possible.

V THE CENSORSHIP ON THE INTERNET

The control on the web set up by the Government is highly sophisticated and provides for mechanisms that allow the authorities and the institutional subjects to watch over the net.

The discipline of the internet providers, both service and contents, consists of a control of contents that takes place in two different moments: the first is an *ex ante* control, through the license system to the providers that, in turn, are compelled to watch over, and censor if necessary, the contents of their web sites (*ex post* control).

Besides this indirect control, the Government has also set up a direct control, through the great national firewall, which intervenes instantly to repress the violations of the regulations. Other technological features allow the authorities to monitor the users' behavior, to filter and to block contents.

In order to explain how the internet censorship system works, we will consider the great national firewall, and the practices of monitoring, filtering and blocking.

But before that, we have to mention the net police, created by the Government, called "big mama", composed of 40 thousands technicians that have to monitor the internet cafes and to install filtering software in web sites, e-mails, BBS and chat-lines. Furthermore, the software Pa-chong, provides for an instant block of sites and users that spread harmful information.

A. The Golden Shield Project

The Golden Shield is the great national firewall, the biggest currently existing in the world. Its complex realization began in 1998, under the supervision of MPS and it has been completed this year. It makes possible a new kind of censorship, which totally differs form the old style one and which is much more effective. It is the instrument that allows the authorities to prevent harmful contents to spread into the net, performing a new and sophisticated censorship. As stated in October 2001 by Greg Walton of the International Centre for Human Rights and Democratic Development: «Old style censorship is being replaced with a massive, ubiquitous architecture of surveillance: the Golden Shield. Ultimately, the aim is to integrate a gigantic online database with an all-encompassing surveillance network – incorporating speech and face recognition, closed-circuit television, smart cards, credit records, and Internet surveillance technologies».[3]

The main part of the firewall is the routers, which manage the traffic of data packets between the networks. Therefore, the networks' administrators can watch over the contents and censor, monitoring, filtering and even blocking specific data when they switch from one router to another.[4] The firewall works mainly at a router level, but this kind of control works only at a national level, because it is only on the web sites which have a national license and not a local one.

The routers employed by the Chinese authorities are provided by the American corporation Cisco.[5]

The firewall has also other technical censorship's features that provide it to control the traffic of information. They are: the blocking of the IP address, the DNS filtering and redirection, the DNS cache poisoning, the URL filtering, the packet filtering, the reset of the connection and the RSS feed blocking. If the technology offers the

[3] In www.ichrdd.ca/english/commdoc/publications/globalization/goldenShieldEng.html.

[4] The routers' censorship is the first level, the ISPs' is the second and the ICPs' is the third. Besides these, we have to mention the license system, the storage of users' data and the principle of the objective responsibility.

[5] The collaboration offered by Cisco has been criticized by a great part of its shareholders who are favorable to more rights-oriented policies. Furthermore, the US Congress has summoned Cisco for a public hearing. See . Critics Squeeze Cisco Over China, in www.wired.com/techbiz/media/news/2005/07/68326 e Cisco Leak: 'Great Firewall' of China Was a Chance to Sell More Routers, in http://blog.wired.com/27bstroke6/2008/05/leaked-cisco-do.html. Cisco has denied any involvement in the Chinese censorship, but there are evidences according to the 2006 China Report of OpenNet Initiative (http://opennet.net/studies/chi) and above all in the internal Cisco's document, available in http://blog.wired.com/27bstroke6/files/cisco_presentation.pdf.

possibility to control and to censor the information, at the same time it provides the net surfers the instruments to bypass such censorship.

The simplest and the more frequent intervention of the firewall is IP blocking, thanks to which the access to certain IP address is denied. If the target web site is hosted in a shared hosting server, all web sites on the same server will be blocked at the same time. This kind of blocking affects all IP protocols (mostly TCP) such as HTTP, FTP or POP. A typical circumvention method is to find proxies that have access to the target web sites, but proxies may be jammed or blocked.

Another kind of intervention is the DNS filtering and redirection that does not resolve domain names or return incorrect IP addresses. It affects all IP protocols such as HTTP, FTP or POP. Against it, a typical circumvention method is to find a domain name server that resolves domain names correctly, but domain name servers are subject to blockage as well, especially IP blocking. Another workaround is to bypass DNS if the IP address is obtainable from other sources and is not blocked.

Again, intervene on the DNS the DNS cache poisoning. It is a maliciously created that provides data to a DNS that did not originate from authoritative DNS sources. This can happen through improper software design, misconfiguration of name servers and maliciously designed scenarios exploiting the traditionally open-architecture of the DNS system. Once a DNS server has received such non-authentic data and caches it for future performance increase, it is considered poisoned, extending the effect of the situation to the clients of the server. Normally, an Internet-connected computer uses a DNS server provided by the computer owner's ISP. This DNS server generally serves the ISP's own customers only and contains a small amount of DNS information cached by previous users of the server. A poisoning attack on a single ISP DNS server can affect the users serviced directly by the compromised server or indirectly by its downstream server if applicable. To perform a cache poisoning attack, the attacker exploits a flaw in the DNS software that can make it accept incorrect information. If the server does not correctly validate DNS responses to ensure that they have come from an authoritative source, the server will end up caching the incorrect entries locally and serve them to users that make the same request. This technique can be used to replace arbitrary content for a set of victims with content of an attacker's choosing. [6]

The URL filtering consists of a scan of the requested URL string for target keywords, regardless of the domain name specified in the URL. It affects the HTTP protocol. Typical circumvention methods are to use escaped characters in the URL, or to use encrypted protocols such as VPN[7] and SSL. [8]

The packet filtering terminates TCP packet transmissions when a certain number of controversial keywords are detected, therefore it affects all TCP protocols such as HTTP, FTP or POP, but when dealing with search engine pages it is more likely they have been censored. Also in this case, typical circumvention methods are to use encrypted protocols such as VPN and SSL, to escape the HTML content, or reducing the TCP/IP stack's MTU, [9] thus reducing the amount of text contained in a given packet.

Quite similar is the connection reset. If a previous TCP connection is blocked by the filter, future connection attempts from both sides will also be blocked for up to 30 minutes. Depending on the location of the block, other users or web sites may be also blocked if the communications are routed to the location of the block. A circumvention method is to ignore the reset packet sent by the firewall.

[6] For example, an attacker poisons the IP address DNS entries for a target website on a given DNS server, replacing them with the IP address of a server he controls. He then creates fake entries for files on the server they control with names matching those on the target server. These files could contain malicious content, such as a worm or a virus. A user whose computer has referenced the poisoned DNS server would be tricked into thinking that the content comes from the target server and unknowingly download malicious content.

[7] A VPN (virtual private network) is a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger network instead of by physical wires. The link-layer protocols of the virtual network are said to be tunneled through the larger network when this is the case. One common application is secure communications through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption. VPNs, for example, can be used to separate the traffic of different user communities over an underlying network with strong security features.

[8] SSL (Secure Sockets Layer) are cryptographic protocols that provide secure communications on the Internet for such things as web browsing, e-mail, internet faxing, instant messaging and other data transfers.

[9] The term MTU (Maximum Transmission Unit) refers to the size (in bytes) of the largest packet or frame that a given layer of a communications protocol can pass onwards. MTU parameters usually appear in association with a communications interface (NIC, serial port, etc.). The MTU may be fixed by standards or decided at connect time.

Lastly, the RSS feed blocking. Recently, due to the great development of the RSS feed, the Chinese engineer have updated the great firewall in order to block also the RSS. Indeed, if an harmful web site is blocked, but not its RSS, the net users could access to the site contents through the RSS. Therefore, since autumn 2007, the great firewall can also block the RSS feed.[10]

The great firewall, due to its highly sophisticated features, provides for what Chinese authorities have called «safe search».

B. *Monitoring*

The monitoring is the simplest among the censorship's systems, but it is surely the most invasive on the users' privacy.

It consists of watching over the internet users, in order to fight the anonymity that characterizes the net, seen by the Government as the major threaten to the State security and social stability. It is conducted through the storage of users' data by ISPs and ICPs.

A particular form of monitoring takes place in internet cafes. The internet cafes are always under control because around 1/5 of the Chinese internet users access the net not through their own pc, but in the internet cafes, making it more difficult for the authorities to control the behavior of every single user.

The 2002 Regulations on the Administration of Internet Access Service Business Establishments (Internet Cafes) have set up a great number of duties the managers have to comply with. Mainly, they have to install in all the pc software that prevent their customers from accessing harmful information and also to keep customers' records for 60 days (art. 23) and do not let the minors enter their cafes. The aim of

[10] http://arstechnica.com/news.ars/post/20071004-chinas-great-firewall-turns-its-attention-to-rss-feeds.html.

these provisions is to urge the managers to do the so called “self police”, looking better after the customers’ use of the net.

C. *Filtering*

In September 2002, a new censorship’s system, based on keywords, was introduced: filtering.

The filtering softwares, installed in every national network, prevent the user to access to particular contents that the authorities consider harmful to national security and social stability. Thus the filtering is a selective censorship, because is based on a list of keywords (as democracy, human rights, Falun Gong …) that would not be displayed by a search engine or in a web site. Therefore, sometimes, you can access a web site containing a blacklisted word, but you can not display the text containing this word.

The filtering system mostly affects the search engines, above all the foreign ones. On the contrary, the Chinese ones are already purged of the blacklisted words. Search engines offer two different kinds of censored results: in the first one, the user is informed that the results are censored, whereas in the second one the censorship is not notified. Baidu employs the second kind, whereas the Western engines prefer the first one. But even in this case, the user does not knows how many results are censored and according to which criteria the censorship is conducted.

It is important to say that the Chinese Government has still not communicated an official list of the keywords that are usually filtered.

Another filtering mechanism is the so called web site de-listing; it takes place when the user types in the search engine the name of a web site and, if it is prohibited, the engine will show no results found. This mechanism is quite similar to blocking; the difference is that in this case blocking is preventive, because it does not even give the possibility to display the URL of the harmful web site, whereas real blocking takes place once the user has typed the URL.

An interesting experiment that shows the effectiveness of the filtering and de-listing of the Chinese censorship is the case of Liu Xiaobo, a Chinese dissident and president of the Chinese PEN.[11] He taped his name, which is in the black words list, in the form of four different search engines: Google.com, Google.cn, Yahoo! China and Baidu. The results, quite surprising, were as follow: 528 thousand results on Google.com, 21 thousand on the Chinese version, 22.900 thousand on Yahoo! China and no results on Baidu.

D. Blocking

The blocking is a kind of censorship that is much more invasive and visible than filtering. It consists of preventing the access not to particular contents, but to particular web sites. Therefore is the IP address or the entire DNS or the RSS feed that is blocked, or instead, the connection is reset.

The web sites that are mostly subject to blocking are the news sites, in particularly Western ones, such as BBC or CNN. The web sites of autonomous regions are also under a strict control, above all Tibet and Xinjian Uyghur, considered by the authorities' possible breeding grounds for political dissent.

As for filtering, the Chinese Government has still not communicated an official list of the sites that are usually blocked.

An interesting case that mixes filtering and blocking concerns the Falun Gong. In February 2003 a team of researchers developed a software called Falun Gong Content Examination System. It provides for an analysis of the contents of web sites

[11] See Liu Xiaobo's interview to the Epoch Times on line on 2006, February 20, available at http://en.epochtimes.com/news/6-2-20/38388.html.

in order to know if they contain reference to the Falun Gong; in this case, if they are pro Falun Gong, the site is blocked, otherwise not.

VI SELF-CENSORSHIP

Another form of control by the Government is the self-censorship. It can be informal or formal.

The informal one is political or psychological. In the first case, the Party and the Propaganda Department issue orders on what matters should be published. On the contrary, the second kind is due to the fear which all the internet operators have to incur in the sanctions provided by the regulations.

The formal self-censorship is the one encouraged by the authorities through voluntary pledges or specific agreements between authorities and providers.

The major example of this second kind of self-censorship is the Public Pledge on Self-Discipline for China Internet Industry[12] signed in 2002 by most of internet providers, both service and content, and also by some foreigners, like Yahoo!. The aim of the Pledge is to «develop vigorously, improve administration, go for its benefits while steering clear of its undesirables and use it to our benefit, in order to establish a self-regulating mechanism for China's Internet Industry, improve the conduct of Internet Industry Participants and promote and ensure the sound development of the Internet Industry consistent with the law» (art. 1). Art. 3 indentifies the basic principles of self-censorship in «patriotic observance of law, equitableness, trustworthiness and honesty». The signers have to refrain from producing, posting or disseminating pernicious information that may jeopardize state security and disrupt social stability, contravene laws and regulations and spread superstition and obscenity; from establishing links to the websites that contain harmful information so as to ensure that the content of the network information is

[12] Text available in www.isc.org.cn/20020417/ca102762.htm.

lawful and healthy; and have to observe laws and regulations concerning intellectual property rights in the course of producing, posting and propagating information on Internet and to encourage people to use the Internet in an ethical way (art. 9). Art. 10 stresses again the importance of inspecting and monitoring information on domestic and foreign websites when it provides access to those sites and refuses access to those websites that disseminate harmful information. Curiously, art. 8 states the need to respect the lawful rights and interests of consumers and to protect the confidentiality of their information.

VII U.S. INTERNET COMPANIES IN THE CHINESE MARKET

Analyzing internet governance in China, it is impossible not to consider the role played by the major US companies in this market. These companies, in order to enter the market and to become competitors with the Chinese ones, have come to collaborate with the authorities, thus limiting the freedom of expression and the right to know and to the information of their Chinese consumers.

The participation of foreign companies to the censorship of the Chinese net is a big problem, in particular from an ethical point of view, because the offer to their consumers is a twisted and not a free service and in so doing they betray the commitments taken with their share-holders, who are, on the contrary, favorable to rights oriented policies. Therefore, governments can take step to increase this regulability[13] and it is important that each national government tries to regulate the activities of their national companies who play roles in countries which offer a censored internet. In this way the Global Online Freedom Act [H.R. 275], a bill of the U.S. Congress, which aims to establish rules of conduct that all US companies that operate in «Internet-restricting countries» have to comply with. They have to document all censorship activities that are compelled to do in such countries (sec. 103); they can not store users' personal data in servers hosted in such countries neither to transmit them to the local authorities (sec. 202). If a US company infringes

[13] Lawrence Lessig, The Law of the Horse: What Cyberlaw Might Teach, 113 Harv. L. Rev. 501 (1999).

the Act, causing one of its consumers to be jailed, it can be sued for damages in front of a U.S. court (sec. 206).

This is certainly an important attempt to set up some rules in the internet business, that can favor a more effective protection of the fundamental rights in the net and a more fair and ethical behavior of companies. Furthermore, Western companies that usually contribute to the diffusion of information and foster the freedom of expression of every single individual could play an important role in promoting the protection of human rights

In this section we will consider the role played by Google, Microsoft, Skype and Yahoo! in the Chinese internet market[14].

A. Google, Microsoft and Skype

The sixth of the ten things Google has found to be true states «You can make money without doing evil». But the Google's role in the Chinese internet market has shown that this is not always true.

Since 2000, Google has provided the Chinese users with a Chinese-language version of its search engine. In September 2002, the Chinese government temporarily blocked Google.com on Chinese internet service providers, making it completely impossible for internet users inside China to access the search engine, thus being automatically re-directed to Chinese search engines. Therefore Google issued a statement to the Chinese authorities calling for the access to be restored; then the block was lifted. However, it was still very difficult for Chinese users to access the Google page and to perform a free search, due to often connection reset.

Google's first step in the direction of compromise with Chinese censorship practices has been the launch of a Chinese-language edition of Google News in September

[14] Human Rights Watch, Race to the Bottom Corporate Complicity in Chinese Internet Censorship, in http://yaleglobal.yale.edu/about/pdfs/china-web.pdf, p. 27.

2004 The Chinese Google News does not display any result for search according to black words. But in this case the filtering is done by the Chinese government and Chinese ISPs, not directly by Google.

Google became an active censor and not merely the victim of State and ISP censorship in December 2005, when it received its license as a Chinese internet service. Thanks to this license, Google could bypass the great national firewall and become a real competitor for the Chinese leader search engine Baidu, but at the same time it had to comply with the strict Chinese regulations on contents. Thus, in January 2006, Google launched a censored version of its search engine for the Chinese market. Tests of the site showed that Google.cn censors thousands of keywords and web addresses, but the “block list” was not given to Google by the Chinese government, but was created internally by Google staff based on their own testing of what terms and web addresses were being blocked by Chinese ISPs. Google de-lists politically sensitive websites from the Google.cn search engine, but does not publicize a list of which sites are de-listed and does not notify the site’s owners. But in all cases in which search results are censored, Google.cn displays a notification at the bottom of the screen. In the future, in accordance to the disclosure policy of informing Chinese users whenever search results have been removed, Google’s new site will provide a link to the uncensored Google.com, still available to Chinese users.

Despite the compromise reached for the search engine, Google has decided not to provide the Gmail and Blogger service to the Chinese users «until we're comfortable that we can do so in a manner that respects our users' interests in the privacy of their personal communications».

In February 2006, Google was called to testify before the U.S. House of Representatives to explain its collaboration with the Chinese censorship. [15] The executives justified their choice saying that «Filtering our search results clearly

[15] For the report of the audition, see http://www.foreignaffairs.house.gov/archives/109/26075.pdf.

compromises our mission. Failing to offer Google search at all to a fifth of the world's population, however, does so far more severely».

Microsoft entered the Chinese market in 1992, but, despite this, the Chinese version of the Microsoft Network (MSN) online portal was launched only in 2005, after the formation of a joint venture between MSN and Shanghai Alliance Investment Ldt. (SAIL) and the birth of MSN China.

Within a month of MSN China's rolling out its Chinese portal, Microsoft came under criticism for censoring sensitive words, at first only in the titles of its Chinese blogs, and then also in the titles of individual blog posts.

In January 2006 MSN launched its own "beta" (test-version) Chinese search engine (at http://beta.search.msn.com.cn). It censors more that Google, but lesser than Yahoo! and Baidu. Concerning searches that have been censored, it often includes a notification to users at the bottom of the page; here the hyperlinked text takes the user to an explanatory page containing explanations of a list of features and potential questions related to MSN search results.

As for the e-mail service, Microsoft has chosen not to provide for a Chinese-language Hotmail service hosted on servers inside the PRC, due to concerns that Microsoft would feel compelled to comply with the local regulation on users' private data transmission to public authorities. In the past, Microsoft successfully refused Chinese government requests for Hotmail user data on the grounds that the data was not under PRC legal jurisdiction.

Just like Google and Yahoo!, Microsoft has been called to testify before the U.S. House of Representatives in February 2006 to explain its collaboration with the Chinese censorship. Microsoft expressed its efforts at transparency while still complying with Chinese censorship requirements, making explicit standards for the protection of content access, maintaining global access – removing access to content only in the country issuing the order – and through transparent user notification in case of content censorship. Microsoft compliance to the Chinese requirement has not been totally condemned. For instance, Zhao Jing, the most famous Chinese blogger, has said that while he would have preferred not to have been censored, it is on balance better that MSN has found a way to compromise, still providing a platform on which ordinary Chinese can speak much more freely than before—albeit not completely freely. [16]

In November 2004 Skype (acquired by eBay in September 2005) launched a simplified Chinese-language version of Skype, jointly developed with TOM Online Inc., a Chinese wireless internet company. In September 2005 Skype and TOM formed a joint venture company to distribute a simplified Chinese version of the Skype.

The Chinese client distributed by TOM Online employs filtering software (ContentFilter.exe) that prevents users from sending text messages with banned phrases and words, thus censoring sensitive words. The text filter operates on the message content before it is encrypted for transmission, or after it has been decrypted on the receiver side. If the message is found unsuitable for displaying, it is not displayed or transmitted anywhere. Skype's executives have justified this as in keeping with local "best practices" and Chinese law. However Skype does not inform Chinese users of the specific details of its censorship policies, neither that their software contains censorship capabilities. We have to point out that the filter operates solely on text chats and not on vocal communications.

B. YAHOO!

Yahoo! was the first major US Internet content company to enter the China market, launching a Chinese-language search engine and establishing an office in Beijing in 1999. In August 2002 Yahoo! signed the Public Pledge on Self-discipline for the Chinese Internet Industry.

[16] Clive Thompson, Google's China Problem, in New York Times Magazine, 23-4-2006, available at www.nytimes.com/2006/04/23/magazine/23google.html?ex=1303444800.

In August 2005, Yahoo! announced it would purchase a 40 percent stake in the Chinese e-commerce firm Alibaba.com. Soon after, Yahoo! merged its China-based subsidiaries into Alibaba, including the Yahoo! Chinese search engine (at http://cn.yahoo.com) and Chinese email service (at http://cn.mail.yahoo.com), leaving the control over what is done in China under its brand name to a Chinese partner.

When in February 2006, Yahoo was brought before a U.S. House of Representatives committee hearing to explain its collaboration with Chinese government censorship requirements, the executives explained that Alibaba.com is the owner of the Yahoo! China businesses, and that as a strategic partner and investor, Yahoo!, and therefore Yahoo! has nothing to do with Yahoo! China collaboration.

Like all other Chinese search engine services, Yahoo! China maintains a list of thousands of words, phrases and web addresses to be filtered and de-listed out of search results. In some cases, searches for some politically sensitive keywords cause Yahoo.com.cn to deliver no page at all in response to the user's request, showing an error message. In other instances they result in server timeout, which causes the entire search engine to be unusable for any search for several minutes. At the beginning, in the search result pages no notice informed the user that the results were filtered; only in 2006, Yahoo! China began showing a disclaimer notice at the bottom of all search pages that some results may not appear, in compliance with the Chinese laws and regulations.

Whereas Google and Microsoft decided not to provide for an e-mail service in order to avoid to be forced to fully comply with the regulations on personal customers' data – disclosing them to the authorities – Yahoo! China made a different choice, providing for a Chinese-language e-mail service. Furthermore, the e-mail accounts are hosted on servers inside the PRC, thus forcing Yahoo! to comply with Chinese regulations and with each request from the public authorities. Indeed, in more than one case (Shi Tao, [17] Wang Xiaoning, [18] Lijun Jiang[19] and Li Zhi[20]) Yahoo, at a

[17] The journalist sentenced in April 2005 to ten years in prison for «divulging state secrets abroad». According to court documents (see www.rsf.org/IMG/pdf/Verdict_Shi_Tao.pdf.) Yahoo! complied with requests from the Chinese authorities for information regarding an IP address connected to a

request of Chinese authorities, has provided them with personal data of customers that used their e-mail address to call for reforms, causing them to be jailed. Analyzing the courts' documents, it is cited as the entity responsible for handing over user data in these cases Yahoo! Holdings (Hong Kong). However, Yahoo! executives insist that the user data for e-mail accounts under the Yahoo.com.cn service were hosted on servers in China, not in Hong Kong. Therefore, Yahoo! claims that it had no choice but to hand over the information, hosted on servers in the PRC.

VIII CENSOR THE CENSORSHIP

The informatics technology can have a dual use: it can be used in order to censor the net, but at the same time to bypass censorship. Besides the filtering software, there are developed to fight the censorship's system of the authoritarian regimes. The main target in fighting this kind of censorship is the possibility to surf the net without being traced and identified, to access to every web site and to freely express opinions in blogs, chat-lines and BBS, getting around filters and blocks. [21]

The simplest way to preserve the anonymity is to use a nickname – but in this case it is still possible to trace the IP address – or to use a public computer. But this is too simple and it is not very effective against the actual censorship, particularly the monitoring that takes place in the internet cafes. Therefore, both the anonymity and the possibility to have access to every web site are not guaranteed.

cn.mail.yahoo.com email account. The information provided by Yahoo! Holdings (Hong Kong) Holdings linked Shi Tao to materials posted on a US-based dissident web site.

[18] The Internet writer and dissident was sentenced in September 2003 to ten years in prison for «incitement to subvert state power», on the basis of essays he distributed on the Internet via e-mail and posted in Yahoo! Groups. According to the court verdict, Yahoo! provided information to the authorities pertaining to the email address and Yahoo! Group used by Wang.

[19] The Internet writer and pro-democracy activist was sentenced in November 2003 to four years in prison for «subversion». According to the court verdict, Yahoo! helped confirm that an anonymous email account used to transmit politically sensitive e-mail was used by Jiang.

[20] The Internet writer was sentenced in December 2003 to eight years in prison for «inciting subversion of the state authority». According to the court verdict, user account information provided by Yahoo! was used to build the prosecutors' case.

[21] Reporters sans Frontières, Handbook for Bloggers and Cyber-Dissidents, in http://www.rsf.org/IMG/pdf/guide_gb_md.pdf.

Another way that provides for anonymity and for free access is the anonymous proxies. In order to use them, it is necessary to accede to a list of proxy servers available in particular web sites, to choose a proxy and then to write down in the internet browser settings the IP address of the proxy and the port listed on the chosen one. The difficulty of this strategy is that in an authoritarian regime every web site containing anonymous proxy lists is supposedly filtered. In any case, even though it is possible to access such web sites, the public authorities can trace the IP address of the internet surfer acceding to them.

The technology provides for other instruments that solve these problems and are able to guarantee anonymous web surfing. The best solution is to hide the IP address using Tor, a very sophisticated network of proxy servers. Proxy servers request a web page on your behalf, which means that the web server does not see the IP address of the computer requesting the webpage. Accessing Tor, three different proxy servers are used to retrieve each webpage. Obviously, these pages are encrypted while transiting between servers. At the same time, Tor installs another software, Privoxy, which increases the security settings of the internet browser, blocking cookies and other tracking software. Tor is a software that has to turn on by hand and every time you want to surfer, which means remembering to change the browser preferences and since it is a multistep process, it is easy to forget to do. Therefore, it is possible to download XeroBank, a highly customized version of the Firefox browser with Tor and Privoxy already installed. It is possible that the web sites providing for Tor and XeroBank to be downloaded are filtered, but in this case they can be downloaded from mirror sites that usually are accessible.

Another recent software developed in Switzerland is Picidae, which is based on an exchange of data. Therefore, if someone has his internet access cut, Picidae will use other points of access, thus never being interrupted. In order to use Picidae, it is necessary to set up "pici" servers, which allow the user to connect to the internet via a computer which is not their own. If the user goes to a "pici" server, a form will come up and he can enter a web address on it. Then, it creates a screenshot of the website and sends it to the user. To make surfing possible from this image, the server will analyze the website and integrate an exact copy with clickable areas instead of links.

In this way all the internet links are then reproduced, like a real web site. Obviously, all the data entered in the forms are encrypted before being sent; therefore, the censorship systems cannot trace the user, nor know what he's researching.

Tunneling uses the same idea as Picidae. The user in a censored location must download client software that creates a tunnel to a computer placed in a non-filtered location. In this way the normal services on the user's computer are available, but run through the encrypted tunnel to the non-filtered computer which forward the user's requests and their responses transparently. Unfortunately, commercial tunneling services sites are known and may already be filtered; furthermore, tunneling software cannot be used on public computers and they may require a higher level of technical expertise.

Quite similar are the so called circumvention technologies. There are two users of circumvention technologies: the circumvention provider and the circumvention user. The first installs software on a computer in a non-filtered location and makes this service available to those who access the internet from a censored location. The problem is that this technology requires a high level of technical expertise and furthermore it can be employed only by the users that have connections in not-filtered countries. A different version is represented by the web-based circumventors. They are special web pages that contain a web form that allows users to simply submit a URL and have the web-based circumventor retrieve the content of the requested web page and display it to the user. Therefore there is no connection between the user and the requested website. When using a web-based circumventor, the end-user does not have to install any software or change any of hid browser settings. All the end-user has to do is visit the URL of the circumventor, enter the URL he wish to visit in the form located on the circumventor page and press the submit button. Thus no level of expertise is required and it can be used from any point of access, even public.

Lastly, we have to mention anonymous communication systems. They are quite similar to circumvention technologies, but they focus more on ensuring the privacy of the user by shielding the identity of the requesting user from the content provider, employing a variety of routing technique. Whereas, circumvention systems do not necessarily focus on anonymity; instead, their focus is on secure communication to bypass specific restrictions. Despite they provide for both security and anonymity, they cannot be used by on public computers and require a high level of technical expertise.

Censorship systems are more and more sophisticated; but we can say the same for the software that allows one to get round the censorship.

IX REFLECTIONS ON CENSORSHIP

The Chinese model is surely a solution to the problem of the internet governance, but it is a solution that infringes some of the fundamental rights of the individual. Due to its effectiveness in controlling the traffic of information and the contents of web sites, e-mails, BBS and chat-lines, the Chinese way to internet governance has become exportable in all the countries characterized by an authoritarian regime, such as Belarus, Burma, Cuba, Iran, Libya, Maldives, Nepal, North Korea, Saudi Arabia, Syria, Tunisia, Turkmenistan, Uzbekistan and Vietnam. [22] Even though these countries do not have the financial resources China has, they have set up a censored version of the net; therefore the web is still not an open space, the filtering software and the blocking prevent the internet users from enjoying their freedom of expression and their right to access to information and knowledge.

If we consider other communist countries, such as Cuba and North Korea, we can see that they have adopted a different way to limit the access to the net and its contents. In both cases, the internet is kept away from citizens. In Cuba, until the recent openness of Raul Castro, it was not commercialized and only the people with a buying license could buy a pc and then have access to the net. In North Korea the situation is quite the same; until 2003 the country was not even connected to the world wide web and now only the political élite can have access to the internet.

[22] For reports on these countries, see OpenNet web site, http://opnennet.net and the one of Reportes sans Frontières, www.rsf.org.

At this point, a specification is needed. The development of filtering software and other systems of control of the internet contents are not evil. What we have to consider is how they are used. The same software used by Beijing, are at the same time used in Western countries, that offer a free version of the net, in order to block obscene, pornographic and sexually explicit web sites.

It means that there are different levels of censorship of the net, and the Chinese way is only one possibility. If we examine the normal practice of different countries, we can identify three censorship models, with a different level of strength: maximum, medium and minimum. The first one is typical of authoritarian regimes, such China, where the freedom of expression and the right to information are totally cancelled. The second is the one used in the major Western countries, because it provides for a selective censorship, which affects only particular contents in front of which the freedom of expression has to be limited. In this case, both the freedom of expression and the right to information are guaranteed, but not in an absolute way, because they encounter limits in values also deserving protection. [23] The third level is based on the *laissez faire* principle, which guarantees at the most the freedom of expression, as stated in the I Amendment of the US Constitution. [24]

X CONCLUSIONS

The Chinese case has showed that a high level of technical expertise and a widespread regulation make possible to realize effective internet governance. Despite it is absolutely necessary to provide for internet governance, it can not be considered the only possible. The internet is a communication media, guarantees the access to the information, is a global forum where everyone can express his opinion; this features should be expanded, not limited.

[23] For example, Google.de has purged its own search engine of Nazi web sites.

[24] See LICRA vs. Yahoo!. In 2000, the US company in front of the Court of Great Instance of Paris in its defense has appeal to the I Amendment. In 2001, the District Court of California, where Yahoo! appealed, has quashed the French decision because in contrast with the I Amendment. However, in 2006, the Court of Appeal of California has doubted the enforcement of the I Amendment outside the US.

The total lack of guarantees of the freedom of expression and the right to information in the Chinese net has been highly criticized by the major dissidents in the Declaration of Citizens' Rights for the internet that recalls both the UDHR and the ICCPR. Indeed, the Declaration has asked the National People's Congress and human rights ONGs to examine the legitimacy and the constitutionality of the Chinese regulations, stressing the importance of the net as an open space.

The reference made by the Declaration to international covenants introduces another problem of the internet governance. Since it is necessary to issue a global governance of the net, due to its trans-nationality, it should be as global as possible. Therefore, besides national measures, should be mainly adopted international ones. But who should be entitled to enact such governance and which is the suitable instrument in order to guarantee freedom of expression, right to privacy and right to information?

The United Nations could be the answer to the first question, maybe creating a special agency charged with arranging an outline of the protection of the human rights on the net. But what should be the better instrument to realize such governance? An international covenant? The problem is whether a covenant, a traditional instrument of international law, is able to deal with a reality as the net that is not traditional at all. Or it should be employed another instrument, expressly established to reply to the challenges of the internet? Personally, I think that a covenant could be the instrument to set up a global governance of the internet, but it should be made as binding as possible, providing for an effective mechanism of warranty against any possible infringement of the fundamental rights. The recent UN attempts to arrange an outline of the internet governance (Geneva, Tunis, Athens, Rio de Janeiro) have not resulted in a great success; no binding covenants have been adopted in these meetings, but merely declarations of intents, in which is favored the adoption of new instruments and mechanism to implement a safe development of the net, respectful of the fundamental rights of the individual. Unfortunately, at the moment, nothing more concrete has followed such declarations. Furthermore, until now, much regulation of cyberspace is conducted by non-governmental entities, that are entities no subject to any of the checks and balances we usually associate with democratic governance in terms of legitimacy, accountability and transparency and therefore the contribution of such entities should be reduced.

The necessity of global governance that protects the freedom of expression is also expressed by the Council of Europe, the EU and the WTO.

Access to knowledge and information is not protected by the Chinese governance of the internet because many Chinese people can not access the net due to the lack of technological facilities and those who have the access are not free to express themselves and they enjoy a service that is censored in its contents. Such barriers to the access should be removed and only an international intervention can guarantee the realization of a true open net society and the protection of the fundamental rights.