Content Filtering in Latin America: Reasons and Impacts on Freedom of Expression

Joana Varon Ferraz, Carlos Affonso de Souza, Bruno Magrani, Walter Britto[1]

Introduction

In December 2010, the Venezuelan Congress approved a bill to regulate access to content and the use of the Internet in the country. The bill was proposed to amend the Law on Social Responsibility in Radio and Television (*Ley de Responsabilidad Social en Radio y Televisión, Resorte*), which already restricts content broadcast by radio and television stations, and attempts to restrict, among other issues, the dissemination of messages that "may constitute media manipulations aimed at creating social unrest or disturbing public order." Under this law, access to websites that distribute messages or information that "may be contrary to national security" or that seek to "discredit legitimately constituted authorities" may also be restricted. Moreover, section 212 of the Resorte Law reform provides that "the Government will create an interconnection or access point to the network of Internet Service Providers in Venezuela for the purpose of handling the traffic originating in and sent to Venezuela, in order to achieve a more efficient use of the networks of the country, given the strategic nature of the sector." Access Providers would be required, since then, to establish mechanisms capable of restricting the dissemination of messages, access to portals and disclosure of information related to the actions subject to the regulations. According to Reporters Without Borders, such a devise would clear the way for network filtering, to the detriment of freedom of information on line.[2] As diagnosed by the NGO Espacio Público, "the project contains serious deficiencies as regards legislative practice as it allows officials who have the responsibility of enforcing this legal instrument to act arbitrarily and discretionarily, which constitutes per se a violation of the human right of freedom of expression and leads to a selective and interested enforcement.[3]

In Mexico, the Party of the Democratic Revolution (*Partido de la Revolución Democrática*) has submitted a bill that intends to monitor and regulate the use of social

[1] Our thanks to Carmen Eugênia Varon for proofreading the text.
[2] http://www.rsf-es.org/news/venezuela-la-ley-resorte-se-extiende-a-internet/
[3] http://www.espaciopublico.org/index.php/noticias/1-libertad-de-expresi/939-ley-resorte-restringe-la-libertad-de-expresion-en-internet-y-medios-electronicos-

networks in the country. According to the bill, the mere exchange of information that helps others violate the law would be considered a crime. Norberto Nazario, the proposer of the bill, defended the creation of an online police force to monitor and hamper the way drug cartels are using the net. Mexican Internet users had a critical reaction to the proposal: many asserted that the law would serve as a mere excuse for the government to increase surveillance; they have even used the term Big Brother to refer to the position the police has sought to take.

Similarly, in April 2011, the Ministry of Justice of Colombia brought a bill before Congress that intends to regulate the Internet and its content. The bill allows ISPs to remove or block access to content *preventively,* in the event someone claims that such content violates copyrights. Civil society has expressed its dissatisfaction with the law, calling it the Hadopi Law, after the French law, which provides a 3-strike procedure to suspend the Internet connection for violation of copyrights. In Brazil, all access to YouTube has already been blocked under a court decision issued within the framework of a process in which a very famous top model was involved. The top model had been exposed in the portal through an amateur video that captured images of her and her boyfriend at the beach, which were at least inappropriate for minors. Though not so recent, the Cicarelli case turned out to be paradigmatic among Brazilian jurists, and started the discussion about why and how to regulate the Internet and protect the rights of access of citizens.

The right of every citizen to seek, receive and share information is protected both in the Universal Declaration of Human Rights and in the International Covenant on Civil and Political Rights (ICCPR). As regards Latin American countries specifically, the Pact of San José, officially known as the American Convention on Human Rights, which was ratified by most countries of the region, lays down rules on censorship in article 13. Similarly, the Tunis Agenda also recognizes these rights within the Information Society, and in item 42 reaffirms their commitment to "the freedom to seek, receive, impart and use information, in particular, for the creation, accumulation and dissemination of knowledge." Most importantly, the same item affirms that:

"measures undertaken to ensure Internet stability and security, to fight cybercrime and to counter spam, must ***protect and respect the provisions for privacy and freedom of expression*** *as contained in the relevant parts of the Universal Declaration of Human Rights and the Geneva Declaration of Principles."*

However, as we have already seen, despite the fact that freedom of expression depends on the free flow of information, there is a tendency for national and regional laws to intervene in the end-to-end architecture of the Internet, prevent the free flow of information and thus undermine the rights of every citizen to freedom of expression and privacy.

It is necessary to closely follow this alleged tendency towards increasing censorship of online information, as several Latin American governments, and governments around the world, have proposed legal texts that impose criminalization of legitimate expressions; liability of intermediaries; and disconnection of users on the pretext of violations to copyright or transmission of illegal information (such as pornography, drug trafficking, cyber attacks, etc.), or that simply establish arbitrary mechanisms to filter, block and remove content from the net and fail to provide an adequate protection of the rights to privacy and protection of personal data.

All these provisions are rather reprehensible, as they not only jeopardize the fundamental rights to privacy and freedom of expression of citizens, but also pose a threat to some of the key elements of the network architecture, such as neutrality and openness. Meanwhile, while developed countries have already established a legal

framework for the Internet, the movement in Latin America is still recent. This context provides more room for reflection, both if we observe the criticisms against foreign regulations, such as the negative reactions to the Hadopi Law, as well as if we strive to evaluate and think of access and freedom-related issues for our specific regional scenario. As the Internet in nature knows no bounds, establishing regulations influences the freedom of access and customs of the other countries; therefore, it is important that developing countries also define standards to be evaluated and discussed globally.

To take advantage of the room left for reflection as regards the future of the Internet in Latin America, this study will explore the laws, court decisions and Internet policies existing in Brazil, Argentina, Chile, Colombia, Mexico and Venezuela,[4] focusing on filtering and content removal cases, and will attempt to evaluate whether the most recent approaches of laws, court decisions and daily practices have been consistent with the guaranteed protection of the right to freedom of expression. This essay is organized in 5 sections: (I) a brief analysis of the meaning of filtering and the fine line that separates it from violation of freedom of expression; (II) a brief analysis of the studies that provide information on the current situation of online freedom of expression in those countries and future trends; (III) analysis of the legal provisions of those countries about (1) access to the Internet service in terms of infrastructure and (2) content regulation; (IV) filtering and the role of the two Service Providers; and (V) Conclusions.

I. The Meaning of Filtering

Just as the advances in technology have led to an unprecedented and immeasurable access to information, technical innovations also provide ways of controlling the flow of that information over the networks. It is necessary to take into account that part of this control has been driven by the need to maintain and improve the quality and security of services in the network, such as by screening out spam and viruses. Thus, the key question is: to what extent is it possible to allow such a control in the flow of information in order to guarantee both the operation of the network as well as the protection of fundamental rights? In addition, efforts are also being made to use that technology to block content that is considered unwanted. In this respect, the second question to be made would be: what is really "unwanted" content? If democracy is based, among other things, on the existence of a space where social or moral criticisms can be made, would those criticisms be considered, in principle, "unwanted"?

According to the UNESCO report entitled "*Freedom of Connection, Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet",* as information and communication flows online, it may use several Internet related protocols and pass through various points in the Internet network until it reaches the user's access devices. Taking this into consideration, according to this report, the most common points at which filtering practices can be applied include:[5]

- Gateways to the Internet backbone: State-directed implementation of filtering and blocking technologies may be carried out at the backbone level, which

[4] We have selected these 6 countries because they are the top 6 in the list of countries by nominal GDP in Latin America (1st Brazil, 2nd Mexico, 3rd Argentina, 4th Venezuela, 5th Colombia and 6th Chile). At first, the selection included only 5 countries. Chile was added to the list because it was the first country to approve a network neutrality law. Cuba was also an interesting option for the subject, but it had to be excluded due to the lack of data available. Even though all the countries will be analyzed, the first version of the essay contains more information on Brazil, given the origin of the authors. We expect to obtain more information about the other countries after the September workshops.

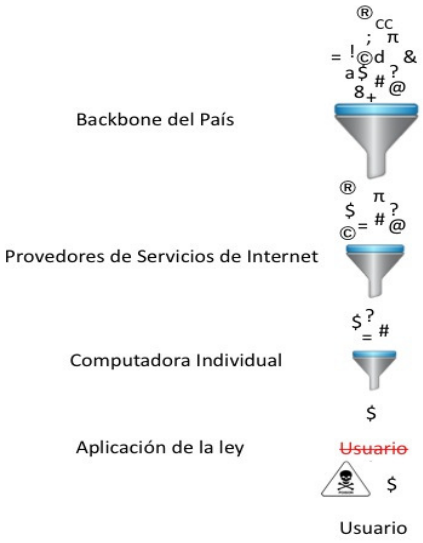
[5] The Locus of Filtering Technologies in UNESCO, "*Freedom of Connection, Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet",* adapted from: Zittrain (2006) and Callanan et al (2009).

constitutes the foundation of the network, such as international gateways in order to eliminate access to certain content throughout an entire country.

- Internet Service Providers: There is a dangerous tendency to have ISPs filter illegal or immoral content, or prevent search results from specified websites. These providers also filter spam and attempt to prevent infection by malware for reasons of stability and user protection.

- Institutions: Companies, libraries, schools, etc. can filter content on the basis of their own criteria and for their own purposes, and/or on the basis of guidelines from state authorities.
- Individual Computers: Each person may install filtering software on their own computer to restrict the ability to access certain content and/or protect their safety.
- Law Enforcement: Actions are also taken against users who engage in practices that are considered illegal on the network, such as fraud, unlawful sharing of music, etc.

1.1 Points at which Filtering Methods are Applied



Source: Prepared by the authors on the basis of the report of the UNESCO[6]

Backbone del País	Backbone of the Country
Proveedores de Servicios de Internet	Internet Service Providers
Computadora Individual	Individual Computer
Aplicación de la ley	Law Enforcement
Usuario	User

Therefore, Internet content can be regulated through those technical approaches implemented at different levels of access to the network. That study seeks to find out, in part, precisely whether the content regulations have clear and reasonable limits for a potential filtering method and whether the filtering methods have taken into consideration at least the legal provisions, or have instead been developed to influence culture and politics by determining which content should be controlled, consumed or produced, promoting excuses such as censorship of political speech, exaggerated protection of copyright, etc.

Most of these practices require some inspection of content, whether to simply identify the identity of the source or even to verify the actual content of the message itself, analyzing all layers of the data packets. Modern technology has developed a mechanism known as “Deep Packet Inspection” (DPI),[7] which is the use of computer systems that enable a third party, not the sender or the receiver of the message, to

[6] Idem
[7] As opposed to “Shallow Packet Inspection,” which is more superficial and only analyzes the packet header.

inspect TCP/IP packets sent over the network. According to Ben Wagner,[8] that mechanism may be "compared to an automated system within the postal service, which opens each letter, checks the contents of the letter and modifies it as necessary, reseals the letter and then sends it on its way."

What differentiates DPI filtering technology is the precision and the scale of traffic that can be filtered, as DPI filtering technology is able to filter the entire packet based on certain properties, such as keywords and size, among others. ISPs and Governments have used this mechanism as a security measure, for example, to combat Denial of Service (DoS) attacks or to manage networks, but this mechanism has also been used to serve the economic interests of non-state actors through service differentiation, behavioural advertising or on the pretext of ensuring enforcement of the law, providing an excuse for surveillance, censorship or monitoring purposes or, worse yet, opening the door for far more subtle censorship methods, as it is said that DPI could lead to a move from filtering internet content to editing it.[9]

As Lawrence Lessig warned, "the design of DPI is not a natural given, but the outcome of political and technological decisions. DPI therefore has the potential to affect the fundamental properties of the internet as a global public infrastructure and therefore also to alter the capacity of global internet governance."[10]

It is important to remember that there are other filtering mechanisms apart from DIP. These include blocking IP[11] addresses or Uniform Resources Identifiers (URI), blocking or manipulating domain name extensions, removing websites from their host server or using other filtering technologies to exclude web pages containing keywords or other specific content from search results.[12] China is the paradigmatic example of the latter, as it has adopted filtering systems that block access to websites that contain such words as "democracy" and "human rights".[13] Finally, it is worth highlighting that all these filtering techniques are not precise, i.e., it is almost impossible to block a specific content without affecting others. However, many of those mechanisms used to regulate and censor information are increasingly more sophisticated and sometimes use many layers of control, which are often hidden from the common user, who will probably not even notice that the information is being filtered. These questions still remain unanswered: Is filtering actually necessary? If so, in which circumstances? What content should be controlled? How? With which transparency measures? The balance between the technical need of filtering practices, the political and social need and the respect for freedom of expression are the topics we intend to approach in our analysis of the policies, laws, court decisions and practices of the 6 countries examined.

II. Brief Overview of Freedom of Expression in Latin America: References to Studies that Map Data of the Current Situation and Future Trends

Before moving on to the comparative analysis of laws, court decisions and cases in the different countries, it seems relevant to briefly map the main studies that have collected information on the issue of online freedom of expression in the region. Our purpose is to understand the political context in which filtering practices are being discussed and

[8] Ben Wagner, Deep Packet Inspection and Internet Censorship: International Convergence on an 'Integrated Technology of Control', Presented at 3rd Annual Giganet Symposium (December 2008). http://www.scribd.com/doc/30663972/Study-Deep-Packet-Inspection-and-Internet-Censorship
[9] Idem
[10] *Lawrence Lessig: Code and other Laws of Cyberspace, New York: Basic Books 1999, p. 32*
[11] Internet Protocol
[12] Frank La Rue Report and Unesco report
[13] Reporters Without Borders, "Enemies of the Internet," March 2010. Available from: http://en.rsf.org/IMG/pdf/Internet_enemies.pdf, pp. 8-12.

take into account the trends in those countries as regards freedom of expression on the net.

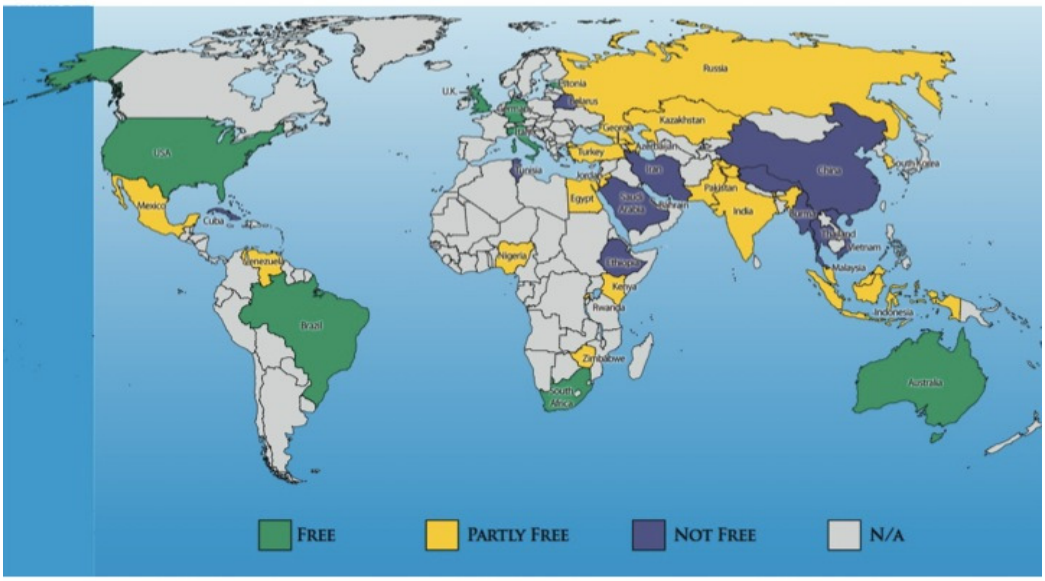
The most thorough and current investigation we have was carried out by Freedom House, in collaboration with the United Nations Democracy Fund (UNDEF). The report "Freedom on the Net, a Global Assessment of Internet and Digital Media"[14] covers developments on the issue of freedom on the net between January 1, 2009 and December 31, 2010. During this period, a series of interviews and surveys were conducted in 37 countries, on the basis of a set of 21 questions and nearly 100 subpoints, organized into three very close groupings, which may be a little broader than those discussed in our analysis:

- Obstacles to Access: including infrastructural and economic barriers.
- Limits on Content: including filtering and blocking of websites, and other forms of censorship.
- Violations of User Rights: including legal protections and restrictions on online activity; surveillance and limits on privacy and prosecution of online activity.

The answer to each question was given a score from 0 (best) to 100 (worst) which allows for comparative analysis among the countries surveyed. After adding the scores of the questions, Freedom House prepared a ranking on freedom on the net. The report is based on the definition of freedom of expression provided by article 19 of the Universal Declaration of Human Rights. Accordingly, the project evaluates the freedom of transmission and exchange of news and other politically relevant communications, as well as the protection of user's rights to privacy and freedom to express their ideas on the net from both legal and extralegal repercussions arising from their online activities. The project considers that only in some narrowly defined circumstances freedom of expression may be restricted, provided that such restrictions are transparent and are implemented in line with international human rights standards, the rule of law, and the principles of necessity and proportionality, all issues that are also highlighted by UN special rapporteur on freedom of expression, Frank la Rue. Thus, countries scoring between 0 to 30 points were regarded as Free; 31 to 60, Partly Free and 61 to 100, Not Free. Rankings of course always lead to questionable generalizations, but the map below allows us to have a global idea of the position of some Latin American countries compared with the rest of the world as regards freedom of expression on the net.

[14] Kelly, Sanja; Cook, Sarah (Ed). Freedom on the Net, a Global Assessment of Internet and Digital Media. Freedom House, April, 2011

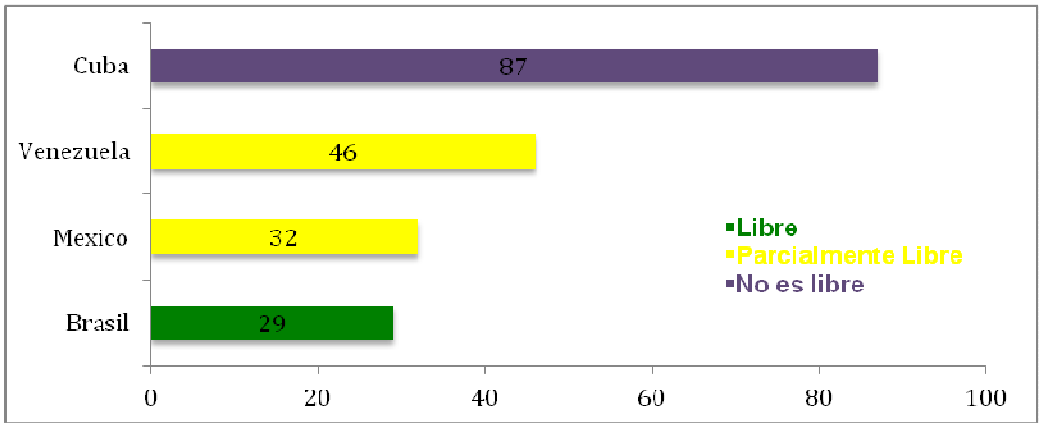
2.1 Global Assessment of Internet and Digital Media



Source: Freedom on the Net 2011, Global Assessment of Internet and Digital Media, Freedom House

As the map shows, as regards Latin America, Freedom House's investigation only includes Brazil, Mexico, Venezuela and Cuba. Only Cuba is identified as a Not Free country, while Mexico and Venezuela show some restrictions to freedom and Brazil respects the possible limits to freedom of expression, compared with the laws and practices of other countries, such as China, Iran, Saudi Arabia and Cuba (which are known to be extremely repressive with respect to this issue, approaching the 100 score to totally unacceptable limits and, therefore, leading to some criticism as to what can actually be considered a free country in the ranking). The graph below shows the scores of each of the Latin American countries that were included in the report, which reveals that there were significant differences between the scores of Brazil, Mexico and Venezuela.

2.2 Online Freedom of Expression in Latin America

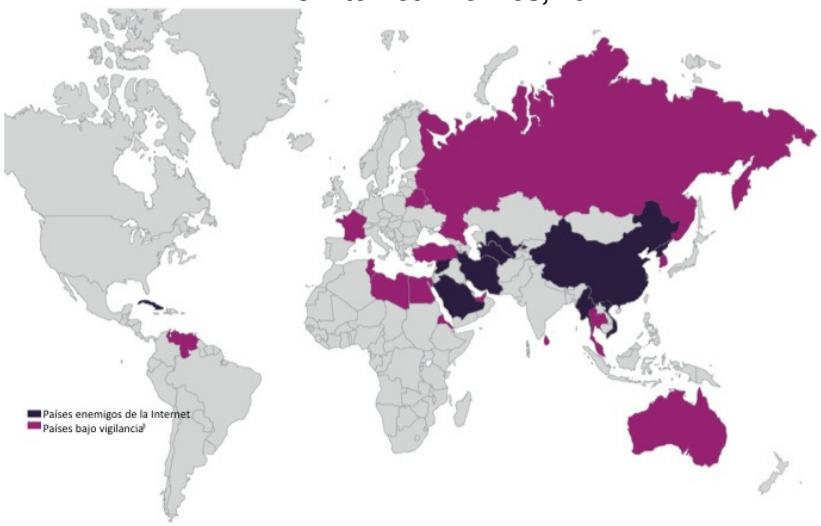


Source: Freedom on the Net 2011, Global Assessment of Internet and Digital Media, Freedom House

Libre	Free
Parcialmente Libre	Partly Free
No es libre	Not Free

With a less refined methodology but based on a survey of empirical cases of censorship on the net, the Reporters Without Borders also published a report in March 2011 where, among the Latin American countries, Cuba was identified as an enemy of the Internet and Venezuela as a country under surveillance, as shown in the map below.

2.3 Internet Enemies, 2011



Source: Reporters Without Borders for Press Freedom, Internet Enemies, March 2011

Países enemigos de la Internet	Enemies of the Internet
Países bajo vigilancia	Countries under surveillance

Even though we do not have final data on freedom of expression on the Internet for the whole of Latin America, Reporters Without Borders has published a ranking on freedom of the press for the whole region. This ranking takes into consideration events between September 1, 2009 and September 1, 2010 and is based on questionnaires distributed among and answered by 178 countries. The study does not look at human rights violations in general, and considers only press freedom violations; i.e., violations directly affecting journalists (such as murders, imprisonment, physical attacks and threats), violations to press freedom in the new media, such as violations of the free flow of information on the Internet, and also the degree of impunity enjoyed by those responsible for these press freedom violations.

2.4 Freedom of the Press in Latin America, 2010

Source: Reporters Without Borders, Freedom of the Press Worldwide in 2010

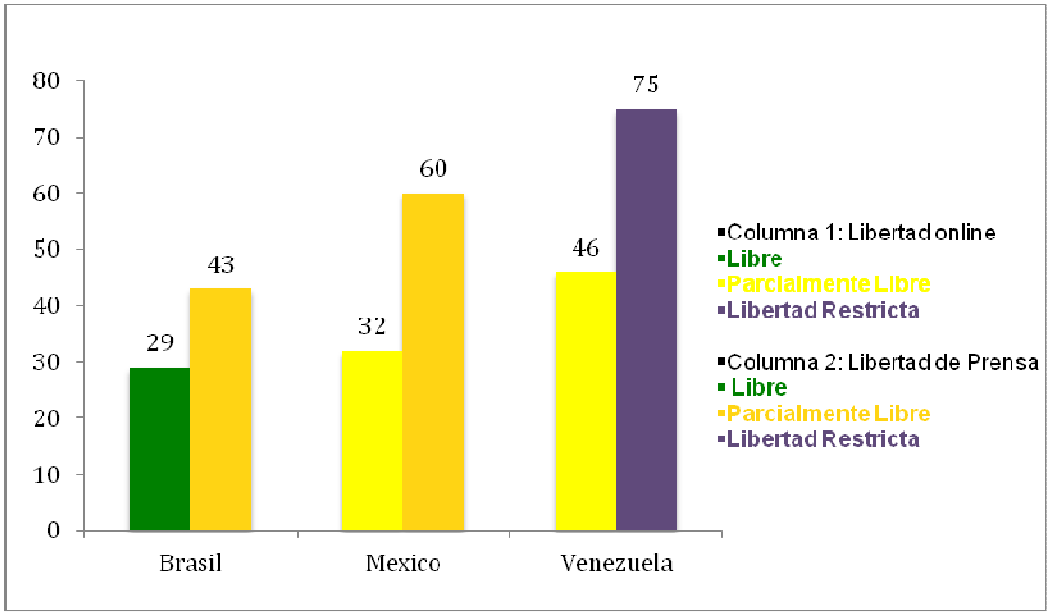
The map shows that none of the countries of the region is in a good situation. Among the countries on which the report is focused, while Chile and Argentina have a satisfactory situation, Brazil has some noticeable problems, and Venezuela, Colombia and Mexico are considered countries in a difficult situation. Cuba, once again, is identified as a country in a very serious situation.

In fact, as the map shows, censorship and freedom of the press are already a matter of concern in the region. As the region increases its Internet penetration rates in the population, we should be watchful to avoid that such a critical profile be extended to the net and to all the other spaces of freedom of expression, which go beyond freedom of the press.

In this sense, interestingly enough, Freedom House's investigation compares its freedom of expression on the net rates with another study, which applied a similar methodology, dealing just with freedom of the press. The graph below highlights that there is a considerable difference in the performance of those countries on the rates of the two studies, with censorship to freedom of the press having still more concerning numbers. As the digital gap is narrowed and the press activities and flow of information

increasingly depend on the net, the question remains whether those high rates of press repression may potentially pose a threat to the future of online freedom of expression in the region. We should keep in mind and closely watch this possible trend, to prevent it from becoming a reality.

2.5 Freedom of Expression on the Internet vs. Freedom of the Press in some Latin American Countries



Source: Freedom on the Net 2011, Global Assessment of Internet and Digital Media, Freedom House

Columna 1: Libertad online	Column 1: Online Freedom
Libre	Free
Parcialmente Libre	Partly Free
Libertad Restricta	Not Free
Columna 2: Libertad de Prensa	Column 2: Press Freedom
Libre	Free
Parcialmente Libre	Partly Free
Libertad Restricta	Not Free
Brasil	Brazil

All in all, the simple lack of investigations about freedom of expression on the Internet with complete data for all the Latin American countries is already worrying. Even though other regions of the world have inspired greater concern for the subject given the existence of serious violations to human rights, we should not ignore what has happened and what may happen in the future of the Internet in Latin America, especially as regards more specific issues such as filtering, privacy on the net and their impacts on the protection of essential rights, particularly in the current context of redefinition of the regulatory frameworks for the Internet in the region.

III. Analysis of Legal Provisions on Filtering Practices

1) Internet Services Access Policies and their Impact on Filtering Practices

Closing the digital divide between Latin American countries and developed countries is still one of the region's major challenge. According to data from the Regional Broadband Observatory (*Observatorio Regional de Banda Ancha, ORBA*), which was launched in May 2011 by the Economic Commission for Latin America and the Caribbean (ECLAC), the percentage of the Latin American and Caribbean population who have mobile broadband services went from 0.2% in 2005 to 4.7% in 2009, while in member countries of the Organisation for Economic Co-operation and Development (OECD), the proportion rose from 5% to 49% in the same period. However, the differences in access in the same countries are also impressive. In Brazil, for example, household access to the Internet among the richest segment of the population is 2% compared to 1.7% among the poorest segment.

Still according to the ECLAC, one of the main factors that determine the take-up of broadband is its price. According to the Commission, in March 2011, the average regional price for fixed broadband was 72.8 dollars per megabyte per second (mbps), compared with 5.9 dollars per mbps in OECD countries, which is a huge difference. This situation constitutes the main obstacle to free access to network content, because it restricts access even before the implementation of any filtering method.

Faced with this situation, all the countries examined are trying to develop regulations that can guarantee the right of access to the Internet service. This is a priority issue, whether because of public policy, or because of the laws that have recently gone into effect or the bills that are under debate. It is worth highlighting that there is still little competition among Latin American Internet Access Providers, which is a common consequence of the not always very well-conducted privatization processes or the existence of state monopoly providers. Therefore, government strategies to expand access can sometimes be contradictory, as some end up giving too much ground to the Internet Service Providers and violating fundamental principles that can ensure a free Internet that respects basic principles to guarantee freedom of expression, such as the principle of network neutrality. That is what we intend to find out in this section, by assessing the policies to ensure the right to be connected and network neutrality.

a) Right to be Connected

Brazil

In recent months, Brazil has established regulations and guidelines to expand Internet access in the country. Even though there is no specific law on the right of access to the net, the Civil Rights Framework for the Internet is in process of approval. This bill intends to establish the rights and duties of users and Internet Service Providers, and among its provisions, section 3 establishes that its purpose is to *"guarantee that all citizens have access to the Internet*." Moreover, Constitutional Amendment Bill No. 6/2011 intends to modify article 6 of the Federal Constitution to read: "*The following are social rights: education, health, food, work, housing, leisure, access to the World Wide Web (Internet)…"*

More specifically, with practical measures, the National Broadband Plan (PNBL) is being discussed, which aims to triple broadband access in the country by 2014, to reach 72% of households. According to the TIC Domicílios report prepared by the Internet Steering Committee (CGI/CETIC), only 27% of households in Brazil have Internet connections, with more than 50% having less than 1 mbps.

Internet access has also been boosted by a proliferation of privately owned "Lan (local area network) houses", in which small entrepreneurs offer Internet access in remote or poorer areas at affordable prices. According to the report published by the Brazilian Internet Steering Committee, Lan houses accounted for 1/3 of the Internet access in

the country, mainly for the people from the lowest income brackets. Unfortunately, those houses have not been taken as the digital inclusion centers they are, and are therefore subject to legal limitations that prevent the access of children and teenagers, and other limitations that make it difficult to operate formally, such as lack of access to loans or incentives to change equipment. However, the scenario has changed slightly and a bill is under debate to create incentives for those entrepreneurs.

Partly on the basis of this information, in recent months the Ministry of Communications has signed agreements to launch the PNBL. While this Plan contains some essential guidelines, it has been criticized for the agreement that the Ministry of Communications entered into with the telephone companies. The agreement establishes a plan of 1 Mps for BRL 35 per month or BRL 29 where state governments waive the ICMS tax (a state value-added tax on goods and services). The Coordination of Social Movements[15] has criticized this agreement, among other things, for not guaranteeing compliance with the 1 Mbps speed (which is considered a low target for broadband connection) and for allowing the joint sale of Internet with a telephone line (which is prohibited by the Consumer Defense Code). Worst of all, telecommunications companies may reduce this speed if the user exceeds 300 Mbytes of download or 500 Mbytes per month. This means that while the agreement creates restrictions for the users on the one hand, it relaxes the rules for the companies on the other.

Also, on June 30, 2011, Decree No. 7512 of 2011 was passed, creating the General Universalization Goals Plan (PGMU)[16], which in section 2–states that the National Telecommunications Agency (*Agencia Nacional de Telecomunicações, ANATEL*) shall adopt, by October 31, 2011, the regulatory measures necessary to establish quality patterns for broadband Internet access telecommunications services, defining speed parameters, service availability and publicity and transparency rules.

In light of this Decree, ANATEL has submitted to public consultation a proposal for massification and improvements to fixed broadband Internet. The public consultation will be held for 30 days, with the aim of having the proposal approved by October 31. According to the proposal, the mean access speed shall never be lower than 60% of what is agreed and that percentage shall be gradually increased. Currently, there is no provision on the subject, and in practice barely 10% is guaranteed. In principle, that proposal only deals with fixed accesses, but ANATEL intends to extend its application to mobile services as well. Users themselves will measure the speed with a software that will be made available by providers. If the proposal is approved, the regulation will go into effect in July 2012.

The regulation also includes provisions on network neutrality, setting forth that “the provider is prohibited from blocking or discriminating against any type of traffic, including voice, data or video, regardless of the technology used.” However, paragraph 1 raises doubts as to the effectiveness of the provision, given that it does not prohibit the adoption of “blocking or traffic management measures that are deemed to be essential for the security and stability of the service and of the networks.”

ANATEL works jointly with the Administrative Council for Economic Defense (CADE) on the basis of cooperation agreements, under the General Telecommunications Law. Their purpose is to ensure that information and communication technologies operate in a free, fair and independent manner. Even though the CADE has the final word under the law when dealing with antitrust issues, such as market concentration and price setting, lack of competition is still problematic in the country. As in most Latin American countries, privatization plans implemented in the 90s created a tendency towards the

[15] Network of civil society associations for a democratic access to the Internet
[16] http://www.planalto.gov.br/ccivil_03/_Ato20112014/2011/Decreto/D7512.htm

concentration of the telecommunications market and ISPs. In an attempt to change the scenario, Anatel also submitted to public consultation the General Competition Goals Plan,[17] for the purpose of regulating competition among service providers in competitive and non-competitive markets. Thus, in the next months, Brazil will certainly have new regulatory frameworks to ensure connection quality.

Argentina

The Argentine government policy as regards the Internet is based on two declarations of principles and is organized around three axes:

The first one is Decree No. 554/97, which declared to be of National Interest that all the inhabitants of Argentina have access to the Internet "in equal social and geographical conditions, at reasonable rates and with quality parameters in accordance with modern applications of multimedia communication." This decree also vests in the Secretary of Communications (*Secretaría de Comunicaciones, SECOM*) the power to develop strategic plans for the expansion of the Internet in Argentina.

Other regulations followed this Decree, such as Decree No. 1293/98, which created the "Internet 2 Argentina" project, and Decree No. 1018/98, which established the Program for the Development of Telematic Communications (*Programa para el Desarrollo de las Comunicaciones Telemáticas*, argentin@internet.todos), for the purpose of promoting the development of the telecommunications infrastructure capable of ensuring universal access. To achieve that objective, the Decree orders the creation of a coordination unit within the SECOM, which will be responsible for planning and assessing the execution of the program. The SECOM is authorized to enter into an agreement with the International Telecommunication Union (ITU) to develop the argentin@internet.todos program.

However, these decrees do not deal with the regulation of telecommunications companies. The privatization of the telecommunications companies in the 90s divided the state company Entel into two private companies, each of whom was assigned a part of the Argentine territory, which afterwards had their shares bought by foreign companies. To ensure investments in modern technology, the government granted those telecommunications companies the monopoly of the basic voice telephone services, in their respective territories. It also granted Telintar the monopoly over international data traffic and inbound and outbound voice. To this day, even though those concessions have finished, the monopoly remains a problem, and ISPs representatives frequently criticize the behavior of telecommunications companies for distorting competition.

Venezuela

Its regulatory framework is based on Decree 825 of May 2000, which sets forth that "Internet is a priority" and declares access to and use of the Internet as political priorities for the cultural, economic, social and political development of the country. Several sections of the decree empower the Ministries to grant financing and tax incentives to anyone who installs or provides goods and services related to the access and the use of the Internet, whether they are government agencies or citizens. The country has also implemented a Science, Technology and Information National Plan (*Plan Nacional de Ciencia, Tecnología e Información*), which establishes certain goals for the 2005-2030 period, including:

"7. To contribute to the creation of an integrated and interconnected Government network, incorporating Internet, voice, data and video access projects."

[17] http://www.anatel.gov.br/Portal/exibirPortalNoticias.do?acao=carregaNoticia&codigo=23243

Meanwhile, the concentration of the amount of Internet accesses in the state-owned telecommunications firm CANTV is still worrying. The Superintendency for the Promotion and Protection of Fair Competition in Venezuela (Procompetencia) has declared that CANTV concentrates around 75-80% of residential Internet accesses. Moreover, the whole capacity of the Simón Bolívar satellite will also be administered by CANTV and the associated Internet services will by provided by that operator. This state control exercised by CANTV over the Internet connection must be highlighted as an important factor that could limit access to certain content and information on the net. CANTV is also planning to install a network access point (NAP) in Venezuela. Those NAPs are points where the networks of the different Internet Service Provider companies converge and through which the traffic between the different ISPs is exchanged. Therefore, they should be administered by an independent company that abides by the network neutrality rule, and not by a single operator that already controls the market.

Colombia

In Colombia, Law No. 1341 of 2009 defined principles and concepts about the information society and the organization of the Information and Communication Technologies (ICTs) in the country, and created the National Spectrum Agency (*Agencia Nacional de Espectro*). Based on that same law, bill No. 149 of 2010 is under debate, which seeks to ensure public access to the Internet. The bill proposes that the Internet should be recognized as a value-added service in section 69 of Law No. 1341, entitled to state subsidies. It also proposes the creation of universal and free-access bands by providing that the "National Spectrum Agency shall identify certain free-access bands that may be used to provide the Internet service, especially in big urban conglomerates." The bill establishes that "said bands may be used by ICT providers at special rates to allow users to address their basic connectivity needs." The Ministry of Information and Communication Technologies also contributed by holding an auction for the 2.5 GHz (gigahertz) broadband spectrum, in order to expand competition and include a fourth company to provide fixed and mobile access services.

Chile

In Chile, a constitutional reform project proposes:

"The freedom and the right to access, on an equal basis, to information, communication and Internet technologies, regardless of the medium used or the geographical location of the users.

A law will determine the way in which the Government will ensure the realization of this right and the conditions of quality and price."

The Ministry of Transport and Communications is planning to reduce the costs of the service by reaching 60% of coverage by 2014 and achieving universal access in eight years.

Mexico

In Mexico, a constitutional reform was proposed to add paragraph 10 to article 4, providing that "every person shall be entitled to have access to the Internet." The government has also recognized its responsibility to plan and promote the development of access to information and communication technologies, which in May 2010 was materialized through the announcement of an investment of USD 115.5 million to extend Internet access to remote areas.

However, in Mexico, just as in the other Latin American countries, a lack of competition in the sector is still contributing to high prices and weakened incentives for the telecommunications companies to invest in the expansion of their services to rural areas. Although there are some independent Internet Service Providers, the company Telmex dominates the market. This is due, in part, to the telecommunications legislation of the country, which was passed in the 1960s and under which the Federal Telecommunications Commission (*Comisión Federal de Telecomunicaciones, COFETEL*) and the Federal Competition Commission (*Comisión Federal de Competencia, CFC*) were tasked with regulating the sector. Press freedom associations have criticized COFETEL for its lack of independence from the Department of Communications and Transportation.
It is important to note that all the countries have started to think of the Internet as a right of every citizen, trying to introduce access policies, some more successful than others, although there seems to be consensus on [sic].

Even though most of the countries analyzed in this study consider that access to the Internet service is a right, we have observed big problems related to the access to the Internet infrastructure and connection quality. But in addition to these technical and economic issues that prevent universal access to the net, there are legal restrictions to access to content.

b) Network Neutrality

As regards access to connection and access to content, the countries examined have shown a tendency to debate laws dealing with network neutrality. Even though it is a technical aspect of network administration, the principle of net neutrality has a clear impact on access to content and may protect freedom of expression, even if such was not its original purpose. To analyze how the network neutrality principle has been implemented and debated in the different countries, we will first briefly describe its general meaning and the basic problem to which this principle refers; then, we will present a comparative chart of how the principle was applied or is being discussed in the different countries included in this study; and finally, we will provide a comparative analysis of the alternatives.

Network neutrality is a principle of network architecture that establishes that all Internet data must be treated equally, i.e., without favoring any application, content or service provider.[18] Thus, it is possible to ensure the free flow of information, without discrimination on the grounds of origin, destination, protocol or content. To implement this principle, Internet Access and Service Providers must transport data packets in a neutral manner, without favoring certain contents and disfavoring others.[19] While Internet providers have no general incentive to discriminate against data packets that are carried through their networks,[20] several studies have shown that access providers have discriminated against traffic at least for three reasons: to increase their own profit, to manage bandwidth on their network or to exclude content that is contrary to the company's policies.[21]

[18] Barbara van Schewick, Towards an Economic Framework for Network Neutrality Regulation, 5 J. on Telecomm. & High Tech. L. 329.
[19] Keeping the Internet Neutral?: Tim Wu and Christopher Yoo Debate.
[20] Se os usuários vêem a liberdade para acessar conteúdos e serviços como um fator agregador de valor ao produto, quanto maior liberdade, maior será o valor do produto para o usuários e consequentemente, mais usuários migrarão para o provedor que oferecer tal serviço.
[21] Barbara Van Schewick and David Farber. Point / Counterpoint: Network Neutrality Nuances.

Frequently, network neutrality is threatened by operators who sign commercial agreements to favor or degrade certain content based on its commercial relationship with the operator. This may happen, for example, with Voice over IP (VOIP) services that may directly compete with an Internet Access Provider that also offers telephone services. Or when an access provider is also a cable TV company and feels threatened by certain online video content, so it slows down the speed at which those packets are delivered. Moreover, on the pretext of traffic management, providers may also discriminate against packets and establish other tiers of quality for a certain service, to the detriment of others, even charging a higher fee, as if imposing a toll on certain types of content, such as more expensive plans to have higher-speed connections specifically for video packets. Some argue that competition policies would ensure that even though providers do not respect network neutrality, the users could choose those that offer the services they need for the fairest price. The truth is, however, that in our countries, in light of what has been explained in the previous section regarding infrastructure and access, and given the lack of transparency in traffic management, there is no level of competition that can guarantee the consumer rights of users. Therefore, the purpose of the network neutrality principle is to guarantee the freedom of the users of the network to access the content, services and applications they choose and to avoid the inappropriate blocking or filtering of content for political or economic reasons, among others.

With respect to these issues, Chile was, paradigmatically, the first country in the world to approve a specific law about the subject. Despite the fact that Chile was the first country to approve that law, the USA had established rules on network neutrality already in 2004, which were laid down by their telecommunications regulatory entity, the Federal Communications Commission (FCC). The FCC's statement established the guiding principles of the telecommunications industry, based on the four freedoms that constitute the central core of any future laws on neutrality. These are: "(a) consumers should have access to their choice of legal content... (b) [should be entitled to] run the applications of their choice... (c) attach any devices they choose [to their broadband Internet access service] and (d) should receive meaningful information regarding their service plans."[22]

To visualize how a significant part of the FCC rules and of the Chilean law has influenced the legislative proposals of the countries examined, we have prepared the following chart. The first three columns of the chart deal with the laws and legislative proposals of Argentina, Chile and Colombia, and are filled with the same color because of the strong influence of the Chilean law. Brazil and Mexico have adopted different approaches and are therefore identified with other colors.

[22] *Notice of Proposed Rulemaking 09-93,* Federal Communications Commission, available at HTTP://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-09-93A1.pdf, accessed on August 16, 2011.

3.1 Comparative Table of Legislations and Legislative Proposals about Network Neutrality in Argentina, Brazil, Chile, Colombia, Mexico and Venezuela

Chile	Argentina	Colombia	Brazil	Mexico	Venezuela
Law No. 18168 of 2010 Section 24 H.- Concessionaires of the telecommunications public utility providing services to Internet Access Providers together with these providers (in the understanding that Internet Access Providers shall make reference to any natural or artificial person providing commercial connectivity services between users or their Internet networks): a) May not arbitrarily block, interfere with, discriminate against, hinder or restrict the right of any Internet user to use, send, receive or offer any legal content, application or service on the Internet, or any kind of legal Internet activity or use. In this sense, they shall offer	**Argentine House of Representatives Bill 1159-D-2011** SECTION 1.- Internet Service Providers, which comprise any natural or artificial person providing commercial connectivity services between users or their Internet networks, and any companies providing connectivity to Internet Access Providers: a) May not arbitrarily block, interfere with, discriminate against, slow down or restrict the use, sending, receipt or offer or any legal content, application or service on the Internet by any user of this service, or any other kind of legal Internet activity or use. b) Internet Service Providers and companies providing connectivity to Internet Access Providers may not limit the right of users to add or use any kind of instruments, devices or equipment on the network, provided they	**Law No. 1450 of 2011** Section 56. Neutrality on the Internet. Internet Service Providers. 1. Internet Service Providers may not, notwithstanding the provisions of Law No. 1336 of 2009, block, interfere with, discriminate against or restrict the right of any Internet user to use, send, receive or offer any lawful content, application or service on the Internet. In this sense, they shall offer to each user Internet access or connectivity, which may not make an arbitrary distinction between content, applications or services on the basis of the origin or ownership thereof. Internet Service Providers may make offers according to the needs of the market segments or their users based on their use and consumption profiles, and this shall not be understood as discrimination. 2. Internet Service Providers may not limit the	**Bill - Internet Civil Framework (*Marco Civil da Internet*)** Section 10. The person responsible for the transmission, switching or routing of Internet traffic has the duty to treat data packets in an isonomic way, regardless of their content, origin and the use of the service, terminal or application, and it is forbidden to establish any kind of traffic discrimination or degradation other than that which would constitute a technical resource necessary to provide appropriate services, in accordance with the regulations issued by the National Telecommunications Agency (ANATEL) about the guarantee of network neutrality and its preservation. Single paragraph. In the provision of an Internet connection, whether as a free service or for a price, it is forbidden to monitor, filter, analyze or supervise	**Bill to amend the Federal Telecommunications Law (*Ley Federal de Telecomunicaciones*)** Section 44 XVI. Where public telecommunication network concessionaires provide Internet access, whether land or mobile-based, they shall ensure unrestricted network traffic and shall abstain from blocking, discriminating against, hindering or restricting the right of users to access, read, send, receive, hire or offer any lawful content, service or application. Internet Access Providers that are not concessionaires but make use of a public telecommunication network shall also abide by the provisions in this paragraph.	None

to each user the service of Internet access or connectivity to the Internet Access Provider, as applicable, which may not make an arbitrary distinction between content, applications or services on the basis of the origin or ownership thereof, according to the relevant Internet connection configuration as per the contract in force with the users. In any case, concessionaires of the telecommunications public utility and Internet Access Providers may take any measure or action that may be necessary for purposes of traffic management and network administration, within the exclusive area of activity that has been authorized to them, provided the above is not intended to conduct actions that affect or may affect fair competition. Concessionaires and IAPs shall endeavor to preserve the privacy of the users, safeguard	are legal and do not harm or adversely affect the network or the quality of the service. c) Internet Service Providers and companies providing connectivity to Internet Access Providers may take any measure or action that may be necessary for purposes of traffic management and network administration, within the exclusive area of activity that has been authorized to them, provided the above is not intended to conduct actions that affect or may affect fair competition. Additionally, they may block access to certain content, applications or services, only upon express request of the users and at their expense. Under no circumstance may this block arbitrarily affect providers of Internet services and applications. SECTION 2.- All ISPs shall publish on their website information about the Internet access offered, its speed (both uploading and downloading speed), and quality of the connection,	right of users to add or use any kind of instruments, devices or equipment on the network, provided they are legal and do not harm or adversely affect the network or the quality of the service. 3. Internet Service Providers shall offer to the users parental control services for content that is against the law, and shall provide users with clear information, in advance, regarding the scope of such services. 4. Internet Service Providers shall publish on their website information about the Internet access offered, the speed and quality of the service, making a distinction between national and international connections, and shall include information about the nature and guarantees of the service. 5. Internet Service Providers shall implement mechanisms to preserve the privacy of the users, protect them against viruses and ensure security on the network.	the content of data packets, except in the cases expressly admitted by law. **ANATEL's Rules and Regulations** Section 59. Internet Access Providers are precluded from blocking or according a discriminatory treatment to traffic of any kind, such as voice, data or video, regardless of the technology used. § 1º A vedação prevista no caput deste artigo não impede a adoção de medidas de bloqueio ou gerenciamento de tráfego que se mostrarem indispensáveis à garantia da segurança e da estabilidade do serviço e das redes que lhe dão suporte. § 2º Os critérios para bloqueio ou gerenciamento de tráfego de que trata o § 1º deste artigo devem ser informados previamente a todos os Assinantes e amplamente divulgados a todos os interessados,		

their users against viruses and ensure security on the network. Additionally, they may block access to certain content, applications or services, only upon express request of the users and at their expense. Under no circumstance may this block arbitrarily affect providers of Internet services and applications. b) Such concessionaires and Internet Access Providers may not limit the right of users to add or use any kind of instruments, devices or equipment on the network, provided they are legal and do not harm or adversely affect the network or the quality of the service. c) Concessionaires and Internet Access Providers shall offer, at the expense of the users requesting it, parental control services for content that is against the law,	making a distinction between national and international connections, and shall include information about the nature and guarantees of the service. **Bill S-1491/11** Section 1.- Telecommunications service providers and Internet Access Providers may not block, interfere with, discriminate against, hinder or restrict the right of any Internet user to use, send, receive or offer any legal content, application or service on the Internet, or any kind of legal Internet activity or use. No hierarchy or priority in the Internet information or services may be established. The quality of the service offered may not be impaired by any traffic management measures adopted. Users may have access to all the content without the intermediation of Internet Access Providers. Section 2.- Telecommunication service providers shall	6. Internet Service Providers shall block access to certain content, applications or services, only upon express request of the users. Paragraph. The Communications Regulatory Commission (*Comisión de Regulación de Comunicaciones*) shall regulate the terms and conditions for the implementation of the provisions of this section. The initial regulation shall be issued within six months following the entry into force of this law.	inclusive por meio de publicação no sítio da Prestadora na Internet § 3º O bloqueio ou gerenciamento de tráfego deve respeitar a privacidade dos Assinantes, o sigilo das comunicações e a livre, ampla e justa competição.		

ethics or moral conventions, provided the user receives clear information, in advance, regarding the scope of such services. d) Concessionaires and Internet Access Providers shall publish on their website information about the Internet access offered, its speed and the quality of the connection, making a distinction between national and international connections, and shall include information about the nature and guarantees of the service. The user may request that the concessionaire or Internet Access Provider, as applicable, deliver such information at its own expense, in writing and within a 30-day term as from the relevant request.	offer to each user the service of Internet access or connectivity to the provider, which may make no arbitrary distinction between content, applications or services. Section 3.- Telecommunications service and Internet Access Providers may take any measure that may be necessary for purposes of traffic management and network administration, exclusively within the area that has been authorized to them, provided the above does not affect fair competition.				

As a supplement to the previous analysis, the table below shows the way in which the general principles laid down in the regulations issued by the Federal Communication Commission influenced the different regulation models for network neutrality in the region.

3.2 Comparative Table of FCC's Basic Freedom Models for Network Neutrality and the Legislations and Legislative Proposals of Chile, Argentina, Colombia, Brazil, Mexico and Venezuela

FCC's Basic Freedoms for Network Neutrality	Chile	Argentina	Colombia	Brazil	Mexico	Venezuela
Freedom of access to any legal content	Section 24, H, a).	Bill 1159-D-2011, section 1, a). Bill S-1491/11, section 1.	Law No. 1450 of 2011, section 56, 1.	Bill - Internet Civil Framework, section 10, heading. ANATEL's Rules and Regulations, section 59, heading.	Bill to amend the Federal Telecommunications Law, section 44.	None[23]
Freedom to run any legal application	Section 24, H, a).	Bill 1159-D-2011, section 1, a). Bill S-1491/11, section 1.	Law No. 1450 of 2011, section 56, 1.	Bill - Internet Civil Framework, section 10, heading. ANATEL's Rules and Regulations, section 59, heading.	Bill to amend the Federal Telecommunications Law, section 44.	None
Freedom to connect any device which does not interfere with the operation of	Section 24, H, b).	Bill 1159-D-2011, section 1, b).	Law No. 1450 of 2011, section 56, 2.	Not included in a specific neutrality provision.[24]	Not included in a specific neutrality provision.	None

[23] See note below.
[24] The fact that this freedom is not contemplated in a specific neutrality provision does not mean that it may not be provided for in another rule.

the network (Carterfone)				Not included in a specific neutrality provision.		
Access to thorough information about service plans (transparency)	section 24, H, d).	Bill S-1491/11, section 2.	Law No. 1450 of 2011, section 56, 4.	Bill - Internet Civil Framework, section 8, IV. ANATEL's Rules and Regulations, section 59, paragraph 2.	Not included in a specific neutrality provision.	None

3.3 Comparative Table of Other Key Issues in the Legislations and Legislative Proposals of Chile, Argentina, Colombia, Brazil, Mexico and Venezuela

	Chile	**Argentina**	**Colombia**	**Brazil**	**Mexico**	**Venezuela**
Is there an exception to the neutrality principle for purposes of technical or security management?	Yes. Section 24, H, a).	Bill 1159-D-2011 Yes. Section 1, c. Bill S-1491/11 Yes. Section 3.	No.	Yes. Section 10, heading. Yes. Section 59, paragraph 2.	No.	Not applicable
Are providers obliged to provide parental control services at the request of users?	Yes. Section 24, H, a).	Bill 1159-D-2011 Yes. Section 1, c.[25] Bill S-1491/11 No.	Yes. Section 56, 3.	No. No.	No.	Not applicable

[25] The section in question does not contemplate the possibility of having the user request a security block from the provider: el bloque de contenidoprevê a possibilidade de que o usuário peça ao provedor o bloqueio de conteúdos de sua escolha, o que pode ser interpretado como permitindo, dentre outros, o controle parental realizado pelo provedor.

2) Content Regulation and its Impact on Filtering Practices

Although access to the Internet has only recently been the object of debate in the laws of the Latin American countries in question, as we found out when we addressed the notion of filtering, legal provisions concerning these issues do not ensure unrestricted access to the content on the Web. Provisions regarding network neutrality do not guarantee such access, either, as they open the floor for legal restrictions to be applied. In view of this, it is important to explore what content regulation laws are about in those countries. First, we need to examine the general freedom of expression guarantees; then, we need to find out what the legal restrictions are and whether these are compatible with the minimum restrictions acceptable for the specific legal system.

Mr. Frank La Rue, the UN Special Rapporteur on freedom of expression, in his report about the promotion and protection of the right to freedom of expression on the Internet, prepared after a series of consultations and meetings held throughout the world, explains that a restriction to online content could be imposed as an exceptional measure "if it passes a three-part, cumulative test:

- it must be provided by law, which is clear and accessible to everyone;
- it must be proven as necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality);
- it must pursue one of the purposes set out in article 19, paragraph 3, of the International Covenant on Civil and Political Rights."[26]

Strictly speaking, this article is one of the most important provisions that should be borne in mind when addressing the issue of filtering and how it should be articulated with freedom of expression. Thus, paragraphs 2 and 3 establish:

> "2. *Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.*
>
> *3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:*
> *(a) For respect of the rights or reputations of others;*
> *(b) For the protection of national security or of public order (ordre public), or of public health or morals."*

That is to say, freedom of expression is not an absolute right and may be subject to legal restrictions provided they are very specific and only to the extent necessary to meet the requirements mentioned before. Additionally, the UN Special Rapporteur holds that any legislation about these restrictions must be applied by a body that is independent of any political, commercial or other unwarranted influences in a manner that is neither arbitrary nor discriminatory; and even so, there should be adequate safeguards against abusive application.

---

[26] Here we could also refer to Article 13 of the American Convention on Human Rights, which regulates freedom of thought and expression and prohibits, in paragraph 2, any kind of prior censorship, and establishes the same tripartite test under article 16 (3) of said Declaration.

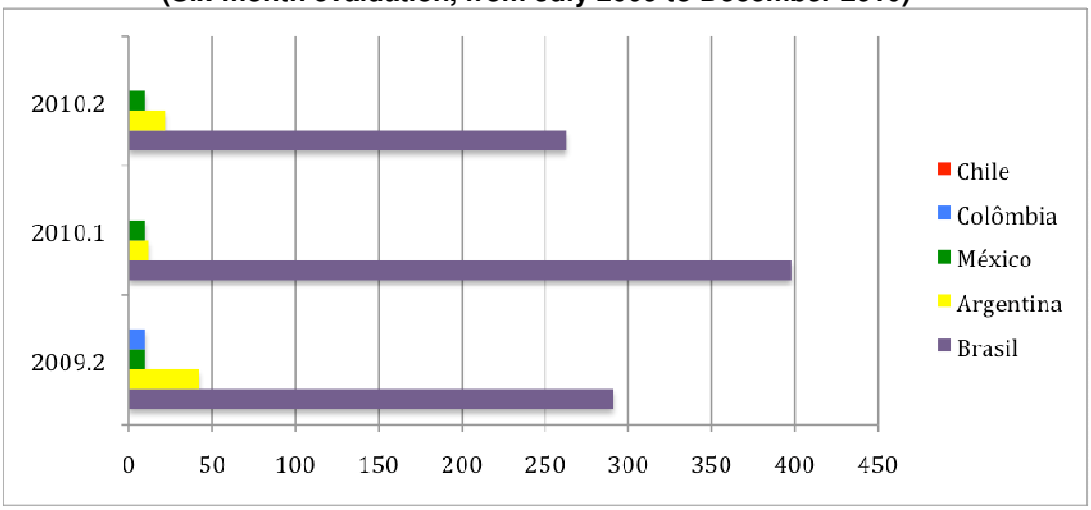
The arbitrary use of the law, for example by penalizing legitimate expressions, constitutes a serious restriction of rights. Taking these requirements into account, we present below a critical examination of content regulations in the countries in question, for the purpose of enquiring whether they truly seek to ensure respect for the reputation and the fundamental rights of others, and protect national security, public order, health and morals in a way that is compatible with freedom of expression. For that purpose, we have divided the analysis into three kinds of content that are usually subject to regulation or filtering practices:

a. Regulation of content that is against equality and the reputation of others: racist and xenophobic content, incitement to terrorism or genocide, hate speech, libel, slander and defamation;
b. Regulation of content that violates copyright;
c. Regulation of sexual content.

An analysis of these regulations and of the way in which they have been used is of utmost importance because, as we discussed in prior chapters, on the one hand the countries in question guarantee right of access and neutrality on the Web, but, on the other hand, the judiciary has played an important role in Latin America in deciding what must be filtered or blocked on the Web, together with the ISPs that receive content removal requests. Sometimes, as we already examined, this is inappropriate and dangerous for freedom of expression.

The chart below displays the information taken from "Google Transparency Report," which shows requests to remove content in Brazil, Argentina, Mexico, Colombia and Chile. Brazil, for example, is at the top of the list among all Latin American countries that requested the removal of content from Google.

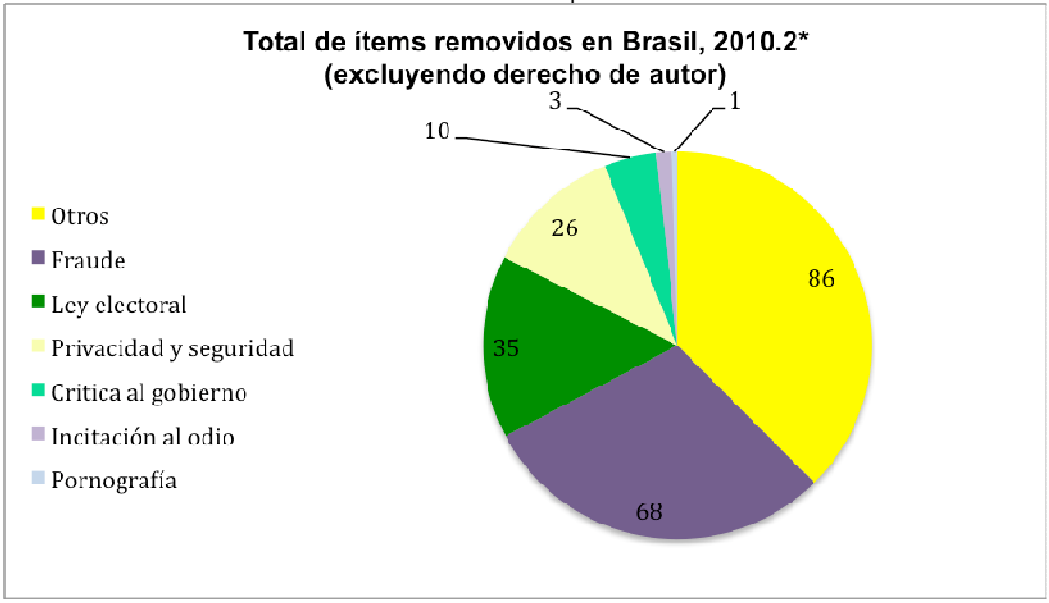
Number of Content Removal Requests from Google
(Six-month evaluation, from July 2009 to December 2010)



Source: Google Transparency Report, available at http://www.google.com/transparencyreport/

Colômbia	Colombia
México	Mexico
Brasil	Brazil

According to the explanation provided by Google, the number of requests for content removal is high in Brazil mainly because of the popularity of Orkut, from where the majority of these requests came. For the most part, these requests related to alleged defamation and impersonation. Of all of Brazil's requests for content removal, the chart below shows the percentage of items removed broken down by reason. According to Google's report, 76% of requests were complied with in the second half of 2010; this amounts to 12,363 items removed from the Internet. Among these, most of them were due to infringement of copyright, mainly in connection with a court order for the removal of 18,000 photos from Picasa. 546 removals related to defamation and were mostly found on Orkut and YouTube. Other cases are presented in the chart below:



Source: Data from "Google Transparency Report."

Total de ítems removidos en Brasil, 2010.2* (excluyendo derecho de autor)	Total items removed in Brazil, 2010.2* (excluding copyright cases)
Otros	Other
Fraude	Fraud
Ley electoral	Electoral Law
Privacidad y seguridad	Privacy and security
Crítica al gobierno	Criticism to the Government
Incitación al odio	Incitement to hatred
Pornografía	Pornography

*These are partial data, as copyright cases are not accounted for. These are much larger and cause graphic distortions; therefore, they render it impossible to make a visible comparison between the categories. The cases represented in the chart did not amount to more than 100 items individually; 11,588 items were removed due to allegations of copyright infringement in Brazil.

a) Removal of Content that Undermines Equality and Reputation of Others

For the purposes of this section, by regulation of content that undermines equality and the reputation of others we understand those regulations that deal with racist and xenophobic content, incitement to terrorism or genocide, hate speech, libel, slander and defamation. We intend to analyze whether the countries have provisions about these topics that are applicable to online behaviors. In cases where regulations address filtering practices, we will examine whether these practices respect

fundamental rights. In the light of these observations, we hope to review whether the decisions taken in the specific cases are consistent with legal provisions and whether they respect freedom of expression.

Brazil

In Brazil, the crime of racism and racial discrimination is provided for in the Federal Constitution, where it is described as a crime that is not subject to any statute of limitations and that does not allow bail. Additionally, the country has a Law on Racial Crimes and the Criminal Code makes provision for slander based on racial, ethnic, religious, nationality or skin color reasons. Last, the Law that criminalizes genocide also includes discrimination issues in the definition of that crime.

When studying these laws in detail, it can easily be gathered that they are also applicable to the actions performed on the Internet. For example, section 20 of the 1989 Law on Racial Crimes, addresses the issue of incitement to prejudice and discrimination by stating: *"Practicing, inducing or inciting to discrimination or prejudice based on race, color, ethnic group, religion or national origin. Penalty: confinement from one to three years and fine."* Such provision sets forth that the punishment may be raised from two to five years and a fine if "*any of the crimes contemplated in the heading is committed through the means of social communication or by a publication of any nature.*" These provisions are a way of penalizing the dissemination of offensive content on any media, including the Internet. They still fall short of being a filtering provision. These kinds of provisions are found in paragraphs 3 and 4 of the same section:

"Paragraph 3. In the cases provided for above, following consultation with the Public Ministry or upon request of the Public Ministry, and even before the police investigation begins, the court may order, under penalty of disobedience:
I - The immediate removal or the search and seizure of all copies of the material in question;
II - The discontinuation of the relevant broadcast on radio or television;
III - The ban of the messages or information pages from the World Wide Web."

Although subsection III of paragraph 3 might be the most apparent one, by construing the language appropriately, it is possible to apply the provisions of all the subsections to cases of discrimination committed on the Internet, even to allow content filtering practices.

The crimes against honor, specified in sections 138 to 145 of the Criminal Code, do not have any reference to banning or removing content, but they do contemplate practices on the Internet as well. Accordingly, section 141, dealing with general provisions, mandates the following:

"Section 141 - The penalties prescribed in this chapter shall be increased by one third in the event any of the crimes is committed:

III - In the presence of several people, or through any means that would facilitate the circulation of a libelous, defamatory or slanderous statement."

Provisions about the way of disseminating these statements are also included in the Law on Genocide (Law No. 2889/56), which criminalizes any direct or public actions or incitement to actions intended to destroy national, ethnic, racial or religious groups. While public incitement is already included in the heading of section 3, paragraph 2 prescribes an increase in the penalty if the press is involved to spread incitement. These regulations leave room for considering Internet practices to be included in them; however, there are no provisions about content filtering.

It is apparent, then, that even if Brazilian law only has one or two legal devices dealing explicitly with the Internet, it can be construed to disallow discriminatory practices or intolerant speech on the Internet. It is worth underscoring that these rules merely seek to prevent discriminatory behavior; filtering practices would be permitted only in the Law on Racial Crimes (paragraph 3, subsections I, II and III).

Meanwhile, there already are decisions about the application of these legal provisions to punish Internet behaviors. These decisions go beyond merely considering these practices as crimes and include the possibility of blocking the slanderous, defamatory or libelous action.

In fact, there have been some convictions on the charge of racism spread on the Internet. The case of Marcelo Valle Silveira Mello,[27] filed in 2009, was the first one to apply the Law on Racial Crimes to Internet-related crimes. The case dealt with a crime of racism which was perpetrated on the social networking website Orkut, in statements against the University quota system for ethnic and racial minorities, which had comments that were highly offensive to blacks. The process was appealed and the second instance Court of Justice of the Federal District and the Territories (*Tribunal de Justiça do Distrito Federal e dos Territórios, TJDF*) convicted the accused by unanimous vote.

Another more recent exemplary case took place in 2011 due to the discriminatory remarks made by Mayara Petruso[28] on Twitter about the people that live in Brazil's North East region. As is well known, Brazil has significant regional inequalities, and it is common for people from other regions to move to the wealthier South East region in search of opportunity. Mayara's remarks gave rise to a wave of prejudiced statements against people from the North East, after the victory of President Dilma Roussef (who is also from that region). Mayara is being tried for racism and incitement to crime.

These are the cases that received widespread coverage by the media, but there were other cases, too; therefore, there is case law about ways to proceed when these crimes are committed. For example, the Superior Tribunal of Justice (*Superior Tribunal de Justiça, STJ*) interestingly found that crimes of racism perpetrated in the same Internet community must be prosecuted in one state of the federation.

In addition to these Criminal Code provisions, crimes against honor are additionally contemplated in the Electoral Code. The Electoral Code has also served as the basis for legal proceedings brought for libel, slander and defamation on the Internet. The language of the Electoral Code sections that define these crimes (sections 324 to 327) is similar to that of the Criminal Code, but is limited to election campaign publicity. Just like in the criminal provisions, in the electoral field an increase in the penalties is also contemplated if "media that facilitate the dissemination of the offense" are used (section 327, III). This, therefore, includes the Internet. Further, these provisions have resulted in the blocking of material in a way that is dangerous and very close to political censorship, as was the case of the political blogs that were taken down during the 2006 elections, at the request of candidate José Sarney, which caused much

[27] "Turma condena acusado de crime de racismo pela Internet" http://www.jusbrasil.com.br/noticias/1845390/turma-condena-acusado-de-crime-de-racismo-pela-internet (accessed on 08/05/11)
[28] "OAB-PE ingressa diretamente com ação penal contra Mayara Petruso" http://www.jusbrasil.com.br/noticias/2716755/oab-pe-ingressa-diretamente-com-acao-penal-contra-mayara-petruso (accessed on 08/05/11)

controversy in the traditional communication media and in the national and international blogosphere.[29]

In the specific case of Brazil, when dealing with content removal by reason of complaints that such content constitutes an attack on the reputation of others, it is important to consider that there are significant records of filtering or blocking ordered by the courts, even though this kind of practice is explicitly provided for only in the Law on Racial Crimes.

As evidenced by Google Transparency Report, among all the countries analyzed in such report, Brazil has the highest number of content removal requests (263 requests), coming before South Korea (139) and Germany (118).

According to the report, the main reason behind the figures being considerably higher than in other countries, in part, is the popularity of Orkut in Brazil. This is due to the fact that, as reported by Google, the platform was subject to content removal requests based on a wide variety of reasons. It should be noted that Brazil is known for the massive use of social networking sites. According to comScore, Brazil is the second country worldwide in terms of number of visits to social networking websites, coming in a close second place to the United States. The last comScore webinar reported that 99 out of 100 Brazilians access social networks at least once a month. While Orkut still leads the preferences of Brazilians, with a 71.9% reach, the use of Facebook is increasing, with 40.8%. Additionally, the country is number six in terms of access to Google+.[30]

If we examine only defamation cases on all Google platforms, 546 items were subject to removal requests. 35 requests were based on Electoral Law reasons, while 3 requests related to hate speech.

Another reason highlighted by Google was the increase in the number of requests issued by electoral courts during the presidential elections, mandating the removal of content related to political campaigns. Unfortunately, there is no information available that is more complete and accurate than Google data, which have some considerable methodological constraints.

Chile

In Chile there are no specific crimes defined for racial issues or other forms of discrimination. However, there is legislation that deals particularly with genocide -Law No. 20357- and anti-terrorism -Law No. 18314/84-. This last law is very controversial in the country, as it is considered to be a remnant of the dictatorship period and is currently used against Mapuche political leaders,[31] thus denying them freedom of expression. In these laws we did not find legal provisions that could be applicable to the Internet, particularly because the laws mentioned pertain to direct physical repression.

On the other hand, two crimes against honor, calumny and insult, are provided for in the Criminal Code in a way that permits its application to the Internet. While the definitions of such crimes are included in sections 412 and 416, section 422 states:

---

[29] "Election and Censorship Dialectics in the Brazilian Blogosphere" http://globalvoicesonline.org/2006/09/01/election-and-censorship-dialectics-in-the-brazilian-blogosphere/ (accessed on 08/08/11)

[30] http://tecnologia.uol.com.br/ultimas-noticias/redacao/2011/04/28/quase-todo-internauta-brasileiro-tambem-acessa-redes-sociais-diz-estudo.jhtm

[31] "Chile: el peso de la ley antiterrorista sigue cayendo sobre los presos políticos mapuche" https://uniaocampocidadeefloresta.wordpress.com/2011/01/27/chile-el-peso-de-la-ley-antiterrorista-sigue-cayendo-sobre-los-presos-politicos-mapuche/ (accessed on 08/05/11)

Section 422. Calumny and insult shall be deemed to have been committed publicly and in writing where they are disseminated by banners or posters placed in public areas; by printed materials that are not subject to the press law, lithographs, printouts or manuscripts circulated among more than five people, or through allegories, caricatures, emblems or allusions reproduced by lithography, printing, photography or any other procedure.

Although the Internet is not expressly considered, it is possible to interpret that online behaviors are punishable under the language of this section that states "any other procedure." However, there is still no knowledge of case law that might have addressed this type of situation; that is to say, it cannot yet be concluded that these laws are fully applied when dealing with the virtual platform. For these crimes, since the application of the laws to the Internet is subject to interpretation, there are no filtering provisions in those cases.

Mexico

Genocide and terrorism are defined as crimes in the Mexican Criminal Code. For genocide, section 149 bis punishes only the commission of the crime but does not criminalize incitement to it. On the other hand, when dealing with terrorism, section 142 establishes that incitement to this crime is also reproachable and is fully applicable to cases where the Internet is used as a communication platform.

Discrimination crimes are provided for in the Federal Law to Prevent and Eliminate Discrimination (*Ley Federal para Prevenir y Eliminar la Discriminación*). Section 9 provides the conditions for freedom of expression in the light of discriminatory behaviors:

Section 9. (...) For purposes of the above, the following are considered discriminatory behaviors:

> *XV. Offending or ridiculing someone or promoting violence in the cases referred to in section 4 of this Law, through messages and images on the mass media;*
>
> *XVI. Restricting the free expression of ideas, preventing the freedom of thought, conscience or religion, or religious practices or customs, provided these do not disturb public order;*
>
> *XVIII. Restricting access to information, except in the cases established by applicable national laws and international instruments;*
>
> *XXVII. Inciting others to hatred, violence, rejection, mockery, defamation, slander, persecution or exclusion.*

Mexican legislation, therefore, includes laws that explicitly address the issue of crimes committed on the Web.

Regarding crimes against honor, Mexico has an interesting example. The country decriminalized these behaviors, which are now subject only to fines and are contemplated in section 1916 of the Civil Code under provisions governing pain and suffering. In cases where damage occurs as a consequence of an action that was communicated through the information media, the solution is even more creative: the law establishes that the court shall order that the media publicize the relevant portion of the judgment or the rectification or response to the information disseminated on the same means of communication where it was published, with the same importance as the original communication." This, therefore, renders it superfluous to have filtering provisions.

Venezuela

In Venezuela there already are more aggressive provisions in terms of filtering of Internet content. The Law on Social Responsibility in Radio, Television and Electronic Media (*Ley de Responsabilidad Social en los Medios de Comunicación de Radio, Televisión y Electrónicos*) is the main regulation on this issue. In section 28 it establishes the guidelines for several limitations to the content of the means of communication, including the dissemination of messages that:

> *1. Incite or promote hatred or intolerance based on religious, political, gender, race or xenophobic reasons.*
> *2. Incite or promote and/or advocate criminal behavior.*
> *3. Are war propaganda.*
> *4. Create social unrest or disturb public order.*
> *5. Discredit legitimately constituted authorities.*
> *6. Lead to homicide.*
> *7. Incite or promote non-compliance with the legal system in force."*

Such a broad legal description of content that must be restricted is an example of a legal provision that clearly opens the floor for filtering practices to be applied.

The way in which Venezuela's Criminal Code describes the crimes of libel, slander and defamation is also very specific; in addition to the general cases committed against any citizen, there is a more specific provision for crimes that are "*in any way offensive to the honor, reputation or decorum*" of the President, the Vice-president and/or members of the judiciary (sections 147 to 151) or the legislative branch (sections 222 to 228). For these specific cases, the penalty consists in imprisonment, while for general cases (sections 442 to 450) there is also a fine. In all cases, penalties are increased "*if the offense is committed publicly,*" which may also include cases of dissemination of offenses on the Internet.

Additionally, regarding filtering practices, it should be noted that section 448 reads:

"In the event there is a conviction for any of the crimes specified in this Chapter, the court shall order the confiscation or suppression of any printouts, drawings and other objects that served for the commission of the crime; if these objects are documents that cannot be suppressed, the court shall order that reference is made on the margin of the relevant documents to the judgment rendered in the case."

Based on this section, it is possible in Venezuela to block Internet content that is considered libelous, slanderous or defamatory if there is a judgment and court order for filtering measures to be taken.

However, the separation between general cases and cases involving the authorities could be a veiled threat, a way to discourage political criticism by the citizens. Recent developments confirm the tense environment in connection with political criticism in Venezuela. For example, a benchmark case in 2010 was the repression suffered by "twitterer" Cristian Fuentes for taking pictures of situations where the Caracas subway was not working well[32] and publishing them in the account @Caracasmetrocuando. While Cristian was taking pictures to post on Twitter, the police detained him and forced him to delete his photos.

Also in 2010, the case of Noticiero Digital became well known as a result of the controversy it aroused between a news website and president Hugo Chávez. In the

[32] "Habla el tuitero del Metro: 'Me detuvieron por hacer fotos del caos cotidiano'" http://www.noticias24.com/actualidad/noticia/178935/habla-el-tuitero-del-metro-me-detuvieron-por-hacer-fotos-del-caos-cotidiano/ (accessed on 08/08/11).

case, the portal called noticierodigital.com, a government opposition forum, was accused by Chávez of having engaged in libel on account of having published false information about the murder of the Minister of Public Works and Housing, Mr. Diosdado Caballo. The news was posted on the website's forum and, as underscored by the company when refuting the accusations, "each user is aware that the messages on this forum are the opinions and expressions of their authors and that they do not reflect those of the forum's administrators or moderators (except for the messages specifically posted by those people). Therefore, under no circumstances is Noticierodigital.com liable for such opinions and expressions." Even though the forum's administrators further stated that the Government was seeking to curb criticism and restrain freedom of expression, as soon as they realized how controversial the posts were, they eliminated them and suspended the users that had posted them. Meanwhile, Chávez demanded that prosecuting attorneys took immediate measures against the website and went even further by requesting more controls over the Internet. These are the President's words:

"The Internet cannot be something open where anything is said and done, right? No, each country has to impose its rules and regulations, just like the TV channels that go in Venezuela by cable, by satellite. This cannot be like that, they cannot broadcast whatever they want, poisoning the minds of many people."

This became a paradigmatic case and a clear example that shows that users do not have clear rights and, thus, they are unprotected. Also, it has served as an excuse for speech that threatens freedom of expression and the Web as a whole. In view of this case, Chávez and his political allies have voiced increasingly harsh criticism to social networking websites, such as Twitter and Facebook, claiming that they are used by their rivals to defame government officials. In this trend, CANTV, the Venezuelan State-owned telecommunications company, announced that it plans to install a centralized filter, which will be controlled by the Government for all Internet traffic. Although Franco Silva, president of CANTV, denied allegations that the measure is going to be used to monitor access to the net, these statements are a matter of concern for advocates of freedom of the press and freedom of expression as a whole.

Colombia

In Colombian legislation, prejudice crimes based on race, ethnic group, xenophobia, etc. are included in the category of crimes of racism and discrimination in general. The Colombian Constitution provides, in Chapter I of Title II, "the fundamental rights" of citizens, and establishes, in section 13, freedom and equality before the law. Under these premises, distinctions among citizens based on "*gender, race, national or family origin, language, religion, political or philosophical opinion*" are considered unacceptable. These provisions are contemplated in the Criminal Code, under title "Crimes against People and Goods Protected by International Humanitarian Law," where section 144 deals with terrorist acts and section 147 addresses racial discrimination acts. However, neither of these sections includes specific provisions about the Web. Further, under the topic of hate speech, the Colombian Criminal Code also makes provision for the crime of advocacy of genocide (section 102), defining it as a crime that is committed "by any real means," including in its definition, of course, the Internet.

What we have seen in Colombia is that the section that lays down provisions about instigation to crime has been used to tackle hate crimes on the Web. Section 348 states that *"any person publicly and directly inciting another person or persons to commit a certain crime or group of crimes*" is a violator. This provision could be applied to discriminatory behavior online. Even though there is no reference to content filtering, in punishing those crimes filtering practices are used, including threats to users.

The most recent case involved Nicolás Castro, a 23-year-old student, who created a Facebook group where he threatened to kill the son of former president Álvaro Uribe, Jerónimo Uribe. Nicolás was charged with instigation to commit a crime, for which he could be sentenced to 6 to 15 years imprisonment. Nicolás was the first Colombian citizen prosecuted for online threats. The proceedings commenced in 2009; in addition to demanding that the web page be taken down, the authorities put Nicolás in jail. The case has stirred up a lively controversy across the country. Although most of the voices on social networks denounce the hatred message attributed to Nicolás, many expressed criticism stating that it would not be sufficient reason for a criminal measure to be adopted. There were many responses that were indignant at the fact that a joke, though reprehensible, can send a young man to prison to serve a longer sentence than that of many paramilitary criminals. It was also highlighted that there are many other Facebook groups that still exist even though they explicitly invite people to kill other people, such as Hugo Chávez, George W. Bush, Diego Armando Maradona, Shakira and other TV characters or members of urban tribes such as the Emos and Punks. Even senator Piedad Córdoba joined in the debate from her Twitter account, explaining that at least 20 groups on Facebook have called on others to kill her, but none of them has been prosecuted33.[32] Nicolás' attorney defended her client advocating the right of expression on social networks. The case is still under analysis.

Colombia also makes provision for the crimes of libel and slander, which are defined in sections 220 to 226 of the Criminal Code. Both prescribe imprisonment and fines which are increased if such crimes are "*committed using any kind of social communication means or any other means of collective dissemination or in a public gathering.*" Additionally, the provisions of section 222 contemplate indirect libel or slander by establishing that "any person who causes the libel or slander committed by others to be published, reproduced or repeated, or any person who makes a libelous or slanderous statement in an impersonal way or using the expressions "it is stated," "it is said," or another similar phrase, shall be subject to the same penalties."

These criminal definitions have been used as the basis for charges against Internet journalists, such as Alfredo Molano[34] -charged with libel and slander for publishing the column called "Araújo et al" in the newspaper El Espectador-, and Claudia López[35] -charged with the same crimes for releasing information about the funding contributed by the Cali cartel to president Ernesto Pizano's presidential campaign-. Fortunately, both were acquitted.

Argentina

Argentine law on hate crimes is mainly based on the Anti-Discrimination Act, signed into Law No. 23592 of 1988. One of the key provisions for our analysis is section 3 which reads:

Section 3. - Anyone who participates in an organization or engages in propaganda based on ideas or theories that uphold the superiority of a race or group of people of a certain ethnicity or color, or who seeks to justify or promote any form of racial or religious discrimination shall be sentenced to one month to three years' imprisonment.

[33] http://www.semana.com/nacion/twitteros-piden-libertad-nicolas-castro-convocan-marcha-facebook/132196-3.aspx

[34] "Juez absolvió al periodista Alfredo Molano en caso de calumnia e injuria." http://www.eltiempo.com/archivo/documento/CMS-7158467 (accessed on 08/08/11).

[35] "Colombia: Jueza absuelve a una columnista acusada de injuria y calumnia." http://www.eleconomista.es/flash/noticias/2857083/02/11/Colombia-Jueza-absuelve-a-una-columnista-acusada-de-injuria-y-calumnia.html (accessed on 08/08/11).

Anyone who encourages or ignites persecution or hate against a person or a group of people based on their race, religion, nationality or political opinion shall be subject to the same penalties.

We might infer that this law prohibits statements based on racism and hatred on the Internet as well. However, interpretations such as this one have aroused a great deal of controversy. This was the case in a judicial discussion that took place in 2000, in which the *Federal Court of Appeals of San Martin, Buenos Aires, found that the sale of Nazi literature or objects* in the auction section of Yahoo! would not be a punishable crime under the Anti-Discrimination Act. Moreover, the offline sale of those materials would not be banned either. Therefore, the Court held that "the auction website does not encourage discrimination or hatred. It only offers for sale objects carrying Nazi symbols, and that cannot be considered illegal."

In practice, such decision was applied in two different ways. Even though the actions in question were not considered crimes under the provisions of Law No. 23592, they were covered by a judicial order for web content blocking issued by the federal judge:

"the Ministry of Foreign Affairs, International Trade and Worship shall be notified of its obligation to make any arrangements as are necessary to prevent YAHOO INC! from showing offers for sale and providing the means for the parties to come in contact, thus participating either directly or indirectly in the process to commercialize and/or promote objects and symbols that rekindle the National Socialist ideas and doctrine, thereby altering the public order and offending the country's morals through the violation of the applicable regulations."

In fact, this decision is also controversial, since the technical staff could not find the way to comply with the court order. The Ministry of Foreign Affairs has informed that there are technical and legal barriers that hinder compliance. On the one hand, Yahoo cannot be banned in Argentina and, on the other, there is the problem of how a decision made by a local court may be applied to a foreign company that stores its information outside the country in question.

In addition to the abovementioned law, in 2005, by means of Decree 1086, Argentina launched its National Anti-Discrimination Plan (Plan Nacional contra la Discriminación), to fight against discrimination, xenophobia and racism. This plan foresees a series of actions to:

"Put in place the mechanisms as are necessary to implement an effective governmental system to follow up and control the form and the contents of the public, private, community and Internet means of communication, including any kind of discrimination, prejudice, mockery, aggression and/or stigmatization of different groups or sectors of the population that, due to their characteristics, may be subject to discrimination."

The plan suggests creating an Observatory of Discrimination in Mass Media governed by the Radio Broadcasting Committee (Comité Federal de Radiodifusión, COMFER) as well as establishing, to such effect, a specific division within the National Institute Against Discrimination, Xenophobia and Racism (Instituto Nacional contra la Discriminación, la Xenofobia y el Racismo, INADI.)

"Create a website content policy aimed at sanctioning Internet providers that host sites with discriminatory and/or xenophobic contents, in order to prevent them from spreading that kind of information."

This is undoubtedly a controversial issue and, as a result, many of the legal provisions in force in the countries examined herein might face challenges. Analyzing this case, we conclude that we may agree or disagree with the authorization to auction items relating to Nazi symbols, but we will probably agree that this involves the risk that, on this basis, requests be then made to block pornographic sites or websites associated with certain religions, or that this could give rise to even more questionable stances. As a consequence, large companies such as Yahoo! would start hosting only "politically correct" sites. This would be a step backwards in terms of the diverse nature of the Internet, which was first conceived as an open space for democratic debate, to make sound decisions and adopt reasonable stances through dialectic processes that analyze the arguments for and against a certain issue. In this regard, in 1997, the president's statement on "Freedom of Expression in the Internet" has accorded a series of constitutional safeguards to the contents shared via Internet because, as pointed out before, there is a thin line between banning of offensive content and censorship.

The regulation of libel and slander in Argentina deserves exploration. In 2009, Argentina passed a series of changes in its Criminal Code, so as to establish lest stringent penalties for those offenses. As a result, under the Criminal Code, slander (section 109) and libel (section 110) are only punished with monetary fines, but not with prison sentences:

> *Section 109: Slander or falsely accusing someone of a specific criminal act which leads to public prosecution shall be punished with a fine from pesos three thousand (ARS$ 3,000.-) to pesos thirty thousand (ARS$ 30,000.-). Expressions referring to matters of public interest or which are not assertive shall not constitute slander.*
>
> *Section 110: Anyone who deliberately damages a person's honor or reputation shall be punished with a fine from pesos one thousand five hundred (ARS$ 1,500.-) to pesos twenty thousand (ARS$ 20,000.) Expressions referring to matters of public interest or which are not assertive shall not constitute libel. Expressions that injure another person's honor shall never be considered libelous when they are related to matters of public interest.*

This is a great step ahead to guarantee the freedom of the press, since it reduces opportunities for disproportionate or unfair sanctions. Nora César, head of the Criminal Law Committee of the Chamber of Deputies in Argentina, defended this notion in an interview with TELAM: "*The freedom of the press is an untouchable pillar of this government. At no time in history has there been such a broad respect for this freedom, which is enjoyed by all journalists.*"[36] The virtual means of communication would enjoy the same protection because, due to the wide coverage accorded by the provisions of the Argentine Criminal Code, the rules on defamation and slander may be applied to the Internet environment.

b.2) Removal of Content that Violates Copyright

The legal protection of copyright has often been invoked as a reason to justify the removal of web content and the implementation of filtering mechanisms. In this connection, it is important to note that the protection of intellectual work may limit freedom of expression.

[36] "Diputados aprobó el proyecto que despenaliza las calumnias e injurias" http://www.telam.com.ar/vernota.php?tipo=N&dis=1&sec=1&idPub=165957&id=322148&idnota=322148 (accessed on 08/09/11).

Most copyright laws in Latin America do not address the protection of intellectual work on the Internet at all, and neither do they establish specific procedures to remove or filter content that infringes copyright on the World Wide Web. Therefore, copyright holders resort to general laws that contemplate the protection of intellectual creations on any means or support to extend the interpretation of those rules to the digital environment.

For instance, the Brazilian copyright law (Law No. 9610/98) provides that the unauthorized distribution of content shall be subject to "suspension of disclosure" (sections 102 and 105), monetary compensation (section 103) and even the destruction of the equipment used to commit the crime in question (section 106.)

In Brazil, copyright protection is enshrined in the Federal Constitution, which states that "authors shall have the exclusive right to use, publish or reproduce their work, and such right may be conveyed to their heirs for the period established by law" (section 5, XXVII.) The Constitution contemplates copyright protection, and this has generated peculiar opinions which claim that copyright protection is an absolute right. However, while on the one hand it is true that copyright must be guaranteed, on the other hand, freedom of expression and other fundamental rights must be analyzed together with copyright protection.

Most cases in which content was removed from the Internet were based on the mere protection of copyright and on absolute repression, without considering how those rights coexist with other fundamental rights, even though there were consistent legal arguments to keep those contents accessible.

Several communities of the social network Orkut, operated by Google, have been blocked or removed as a result of extrajudicial claims alleging that their presence on the Internet was a personal infringement of copyright. One of the most prominent cases was the removal of the "Discography" (Discografía) community, which suggested links to download songs and albums in MP3 format.[37]

Even when they abide by copyright laws, the sites that reproduce subtitles for serials and movies have received extrajudicial notices. The case of the website "legendas.tv" clearly illustrates how the extrajudicial notice mechanism has helped restrict the posting of content that could be easily challenged as illegal based on copyright limitations and exceptions.[38]

The notice regime has been subject to thorough examination as a result of the Bill to Amend the Copyright Law in Brazil. In section 105-A, this bill provides that the hosting service provider shall be jointly and severally liable if it fails to prevent access to the allegedly illegal content after having been notified by the injured individual. The bill reads as follows:

Section 105-A - Anyone who provides hosting services for Internet content may be held jointly and severally liable, pursuant to section 105, for damages resulting from public disclosure of works and phonograms without authorization by the owner, if following notice by the injured owner, said provider fails to take necessary action to make the harmful content unavailable through their service and within a reasonable term.

In contrast to the Brazilian scenario, Venezuela has passed a Law on Information Technology Crimes that sets forth the penalties for online conduct which is considered illegal, including in its provisions on intellectual property:

[37] http://www1.folha.uol.com.br/folha/informatica/ult124u535222.shtml (accessed on 08/19/2011).
[38] http://idgnow.uol.com.br/internet/2009/02/03/apcm-pede-retirada-do-site-legendas-tv-do-ar-por-infracao-de-copyright/ (accessed on 08/19/2011).

> *Section 25.- Misappropriation of intellectual property. Anyone who, lacking authorization by the author and for the purpose of financial gain reproduces, modifies, copies, distributes or makes available to the public a piece of software or any other piece of intellectual work that may have been obtained by accessing an information technology system shall be sentenced to one to five years' imprisonment and shall be fined an amount equal to that represented by 100 to 500 tax units.*

The application of criminal law to copyright infringement is justified by the fact that the provisions of criminal law are very specific and, as a general rule, do not allow for analogies. Given the fact that the penalties imposed by criminal law are harsher than those applied by civil law and provide for imprisonment sentences, criminal law has become widely used to prevent copyright infringements and this has indirectly promoted content filtering practices.

The Colombian Constitution establishes that "*The State shall protect intellectual property for the term and pursuant to the formalities prescribed by the law"* (article 61.) As a member of the Andean Community (Comunidad Andina), the country is a signatory to the Common Regime on Copyright and Related Rights (Régimen Común sobre Derechos de Autor y Derechos Conexos) (Decision 351 of 1993), which accords authors a wide set of rights. Its Copyright Law (Ley de Derecho de Autor) (Law No. 44 of 1993) supplements this Regime and incorporates penalties for copyright infringements, including:

> *Section 55.- Any confiscated publications, copies, reproductions, casts, sheets, matrices, negatives, tapes, covers or labels shall be subject to judicial examination with the assistance of a relevant expert. After proving the illegitimate nature of those materials, they shall be destroyed by the criminal investigation authorities, before a court officer, and having summoned the defense and the plaintiff.*

The Colombian Criminal Code addresses the protection of authors' moral and property rights in sections 270 and 271, and the protection of the mechanisms to defend those rights in section 272. It refers to technical and technological mechanisms to protect data stored in computers, on the Internet and on satellite television, emphasizing the possibility of using those mechanisms in the digital environment.

In 2008, the Supreme Court of Colombia, in a case involving the copying of pieces of musical work, issued a landmark decision on the disclosure of copyrighted material via Internet. Regarding this decision, Carolina Botero states:

> "The precedent created by this decision does not lack significance: it sets forth that, where no financial gain is sought, copying materials shall not constitute a crime. It also limits the scope of the "intent to profit." By establishing a link between this concept and an economic scale, it acknowledges the importance of exceptions and their applicability in the criminal sphere as a subjective element of the crime that the judge must take into account. This ruling states that the mere "use" of software without a license is not a crime. Although the reference to materials downloaded from the Internet is only made by way of example, this confirms that other judges should at least consider this issue when they hear similar cases."[39]

[39] "equinoXio: La Corte Suprema de Justicia sienta precedente sobre "ánimo de lucro", "uso personal", etc." http://www.karisma.org.co/carobotero/index.php/2008/05/09/equinoxio-la-corte-suprema-de-justicia-sienta-precedente-sobre-animo-de-lucro-uso-personal-etc/ (accessed on 8/10/11).

Chile put in place an important amendment of its Copyright Law. Harsher penalties and fines for copyright infringements were established and, at the same time, mechanisms to prevent arbitrariness and prior censorship were also created. Hence, at present, Internet service providers in Chile are not fully liable for the content that their users disclose on the Internet, and content filtering may only be implemented by a court order.

Over the last years, the regional scenario has been marked by the adoption, by Latin American countries, of solutions implemented by European or North American countries to combat copyright violations. In this regard, practices such as the interruption of the Internet service following receipt of a notice of copyright infringement, such as the Hadopi Law in France, were introduced in draft legislation in Latin America.[40]

In Brazil, for example, a bill authored by the federal deputy Bispo Gé Tenuta proposed cutting the Internet connection after serving notice of an alleged copyright infringement for the fourth time. This bill, No. 5361/2009, raised a great deal of controversy and it was finally dismissed. In the deputy's words, discussions pointed out that "it would be impossible to differentiate between those who profit from piracy as a business and the youngsters who use Internet to listen to music, as we did in the old days, when we recorded radio broadcasts on a cassette tape."[41]

This statement shows how content filtering for copyright protection may negatively affect freedom of expression and access rights, to the extent that it would impact on legitimate situations and it would give way to a poorly defined repression which may be counterproductive.

c) Removal of Sexual Content

Brazil

The Brazilian law addresses offenses to decency in its Criminal Code. Section 234 criminalizes the sale and public exposure of an "obscene object" as a crime constituting a less serious offence. However, we should not lose sight of the fact that a behavior that is common in a certain community may not at the same time be considered relevant for Criminal Law purposes. With regard to this provision, legal authors have considered that the Federal Constitution (Constituición Federal, CF) adopted after the dictatorship guarantees freedom of expression, and so this prohibition may not be understood in terms of punishment. In fact, based on the changes in social customs, even before the adoption of the Constitution of 1988 such crime was seldom punished. After the abolition of censorship by article 5, IX of the Federal Constitution, the definition of this crime is almost ineffective, or otherwise, all movie theaters showing pornographic films, sex shops, magazines or TV channels with pornographic material would be prohibited. All these materials and business activities are tolerated by society and authorized by the Government, and they are even subject to taxes. Therefore, the case law on the subject provides that the conducts in question should not be punished, considering that the legally protected interest, i.e. the common conception of decency, has changed substantially. The prevailing social values are no longer consistent with such provision, and this constitutes a supra-legal ground to exclude the definition of the crime which has been accepted by both modern doctrine and case law. Such reasoning applies also to the posting of pornographic content online.

[40] http://www.senat.fr/leg/pjl07-405.html (accessed on 08/19/2011).
[41] http://www.trezentos.blog.br/?p=2752 (accessed on 08/19/2011).

But of course, there is another question related to pornographic content that must be categorically rejected by society: child pornography. This topic is addressed in the Children and Adolescents' Charter (Estatuto da Criança e do Adolescente - ECA) (Law 8069/90.) This charter was amended by Law No. 11829/08, to specifically contemplate cases relating to the Internet. Thus, sections 241 to 241-C set forth the penalties to be applied to different crimes associated with child pornography over the Internet as well as in other means of communication.
The law establishes a system which holds every participant in the pornography chain liable. Besides punishing those who produce, record or manage the illegal contents, it penalizes individuals who coordinate, facilitate, recruit, coerce or otherwise act as intermediaries to have the child or adolescent participate in pornographic scenes (section 240, paragraph 1.) Those who sell, expose, publish, distribute, purchase or store this type of images are also criminalized.

Regarding provider liability in particular, paragraph 2 of section 241-A stipulates that anyone who facilitates access to or storage of illegal content shall be liable, providing that:

"the person in charge of service provision, having been duly notified, fails to disable access to the illegal content referred to in the section heading."

It is important to note that such law creates a filtering mechanism that is relatively balanced with respect to freedom of speech, as it requires that the provider be given prior notice to be held liable. Therefore, it does not impose any kind of "a priori" restriction forcing providers to monitor all the content in their network, which would constitute a serious violation of user privacy. However, this law charges them with the obligation to withdraw the illegal content.

Moreover, the law sets forth a reporting mechanism. Those who store illegal content to enable access by the relevant authorities are not considered offenders and must treat the material in question as confidential. In addition to the criminal action pursued by the Public Ministry, this type of offenses could also be reported via Safernet, a private law organization that cooperates with public institutions.

Although this law provides mechanisms which are accurate and appropriate for their intended purpose, there is also the intention to extend the scope of provider liability. Bill No. 494/08, drafted by the Parliamentary Committee of Investigation (Comissão Parlamentar de Inquérito, CPI) on Pedophilia, seeks to hold access providers liable irrespective of whether they have been given prior notice or not. In our view, the above regulations would impose a heavy economic burden on providers and may endanger innovation in the web. Besides, we understand that the applicable laws already afford considerable protection to this issue. Even though this is an extremely sensitive issue of utmost importance, all the rights to be protected must be given equal consideration. In Brazil, the fight against child pornography over the Internet is already supported by a series of laws that regulate its availability online. This is proven by a number of successful operations based on ECA, for instance, operations Carrossel I[42] and Carrossel II[43], in which the Federal Police executed judicial orders for search and arrest pursuant to section 241 et seq.

[42] "MPF/BA: economista é denunciado por disponibilizar via internet materiais de pornografia infantil" http://noticias.pgr.mpf.gov.br/noticias/noticias-do-site/copy_of_criminal/economista-e-denunciado-por-disponibilizar-via-internet-materiais-de-pornografia-infantil (accessed on 8/6/11).
[43] "Operação Carrossel II combate pornografia infantil pela Internet" http://www.safernet.org.br/site/noticias/opera%C3%A7-carrossel-ii-combate-pornografia-infantil-pela-internet (accessed on 8/6/11).

It is worth pointing out that Safernet, the same organization that has been exerting pressure to adopt a new legal framework, has recently faced termination of its technical cooperation contract with the Federal Public Ministry (Ministério Publico Federal, MPF) in Sao Paulo. This authority stated, in a technical communication released in November 2010, that the organization is unable to process and analyze the notices submitted by Internet users through the central unit for complaints, with national coverage, maintained by the NGO. Now that this partnership has been dissolved, user complaints must be submitted via the Digi-denúncia system. The prior agreement stipulated that the reports were to be received by Safernet. This organization was supposed to identify the links in question and then pass this information on to the relevant authorities. According to the MPF, a total of 40,000 reports were received. Among them, the technical staff of the MPF found 27 evidences of serious crimes that had not been referred to this authority by Safernet. This shows that, apart from legislative changes, there is a need to review the institutional structures in charge of investigating complaints.

Venezuela

Venezuela has set up a comprehensive legal surveillance system over activities involving pornographic material on the Internet. This issue is regulated by three different laws: the Special Law on Information Technology Crimes (Ley Especial contra los delitos informáticos), the Organic Law on the Protection of Children and Adolescents *(*Ley Orgánica de Protección al Niño, Niña y del Adolescente, LOPNA) and the Law on the Protection of Children and Adolescents in Establishments for the Use of Internet, Videogames and other Multimedia Systems (Ley para la Protección del Niño y del Adolescente en Salas de Uso de Internet, Videojuegos y otros Multimedias.)

The first of these laws sets forth the basic rules for pornographic activity over the Internet. According to section 23, any dissemination of pornographic material requires a prior warning on the content. The following provision, section 24, specifically seeks to repudiate child pornography by penalizing the pornographic exhibition of children or adolescents in the web.

LOPNA establishes children's fundamental rights and obligations. For example, section 33 refers to the right to be protected against abuse and sexual exploitation. Together with section 24 of said law, these are the only legal provisions on child pornography applicable in the country. The other provisions deal mainly with the sort of content that may be accessed by children. Similarly, sections 74 and 79 of LOPNA establish prohibitions to prevent children from accessing certain improper content. So does the law that regulates establishments offering Internet access, which provides that Internet services must be used for education purposes and stipulates the required filtering systems that should be applied in such premises.

Section 10. This section stipulates that all the establishments offering computer, electronic or multimedia games, as well as those offering Internet access, must implement specific control devices, safety mechanisms and software in the computers and equipment to be used by children and adolescents, pursuant to the provisions of the law. It also sets forth that Internet service providers shall supply all their users with free control devices, software and safety mechanisms.

Colombia

In 2009 Colombia approved, by means of Law No. 1336/09, a number of legal amendments (Law No. 679 of 2001 and Law No. 599 of 2000) to fight exploitation, pornography and sex tourism involving children and adolescents, including the commission of these crimes via the Internet. Thus, section 218 of Law No. 599/2000, as restated, provides that anyone who

"takes photographs of, films, records, produces, discloses, offers, sells, buys, possesses, carries, stores, transmits or exhibits, by any means, for personal use or exchange with others, real representations of sexual activity involving an individual under 18 years of age" shall be considered to be engaged in pornographic activities with individuals under 18 years of age.

Based on this definition, Law No. 1336 introduces a new paragraph to section 10 of Law No. 679/01. The heading of this section authorizes the Ministry of Communications to intervene in these cases by processing complaints and exercising the authority to impose fines and block websites. The new paragraph empowers the Ministry of Communications to require from Internet service providers any information deemed necessary to prevent and counter exploitation, pornography and sex tourism involving minors, and specifically addresses filtering rules by providing that the authorities shall have power to:

"1. Require Internet service providers to disclose, in the manner and within the period specified, the mechanisms or filters that they use to block pages with pornographic content involving minors.

2. Require Internet service providers to include mandatory clauses in their Internet portal contracts relating to the prohibition and subsequent blocking of pages with pornographic content involving minors.

Internet service providers shall grant judicial and police authorities access to their networks so that they can track an IP number when the law is infringed."

In addition, like Venezuela, it also refers to Internet cafes and provides that those sites shall adopt a set of appropriate public access regulations that, if infringed, will result in the suspension of the service for the user or guest.

Argentina

To date, Argentina has not passed any specific laws relating to child pornography over the Internet or pornography in general. There have been, however, local efforts to regulate this issue. This is the case, for example, of the city of Buenos Aires, where municipal Law No. 451 provides as follows:

Section 1- Any commercial establishment offering Internet access in the Autonomous City of Buenos Aires shall install and enable content filters for pornographic sites in all the computers available to the public.

Section 2- The owner or person in charge of the establishment may disable the content filters in their computer equipment when users are over 18 years of age. (Pursuant to Section 1 of Law No. 943, Official Gazette of the Autonomous City of Buenos Aires [BOCBA] No. 1604, dated 01/08/2003.)

This shows that Argentina addresses child protection in the same way as other countries do, i.e. by putting in place filtering mechanisms. It is important to note that this law refers to Internet cafes, whereas Federal Law No. 25690 sets forth that providers shall furnish users with filters that they can easily configure after deciding for themselves what contents they do not wish to access. This is an interesting and less restrictive solution, which respects the web structure as well as child protections by means of user self-determination.

Chile

In Chile, the main legal framework for the regulation of pornography in the web is Law No. 19927 of 2004 amending the Criminal Code, the Code of Criminal Procedure and

the criminal procedure for child pornography crimes. Section 366 was amended as a result of the changes introduced by the law:

"Anyone who engages in the production of pornographic material, irrespective of the supporting media used, involving individuals under eighteen years of age, shall be punished with the maximum duration established for short-term imprisonment.

It is clear that the expression "*irrespective of the supporting media used*" includes child pornography over the Internet within the scope of the law. In addition to this law, there are other bills in the pipeline, including one that seeks to introduce provisions relating to "grooming" and "morphing" in the Criminal Code: these are forms of seduction and abuse of minors that are necessarily based on the Internet.

Although the investigation agency in Chile has a unit dedicated to fighting sexual crimes which monitors child pornography websites and prosecutes individuals who sell, store or exchange child pornography over the Internet, there are no reports indicating that the government monitors e-mails or chat rooms for other purposes.[1]

Mexico

Mexico also deals with child pornography straightforwardly in its Criminal Code. Under section 202, an offender is "*anyone who forces, helps or induces, by any means, one or more people to engage in sexual or indecent exposure activities for prurient or sexual purposes, either real or simulated, in order to make videos and recordings, take photographs, film, exhibit or describe those activities in print advertisements, data file transmissions on a public or private telecommunications network, computer or electronic systems or any other similar means.*" Therefore, the Internet may be included among the tools used to commit the crimes in question. Not only dissemination, but also storage of those materials is prohibited:

> *Section 202 BIS.- Anyone who stores, buys or leases the above materials without commercialization or distribution purposes shall be sentenced to imprisonment of one to five years and shall be subject to 100 to 500 daily fines. They shall also receive special psychiatric treatment.*

At present, no determination has been made on content filtering; the law only imposes a sanction for making the contents available and/or for storing them.

IV) The Role of the Two Service Providers[44]

The debate on the effects of filtering mechanisms may not leave aside the role of service providers and the problems that their implementation raises in practice, especially when the use of a filter is required by court order. Finally, this part of our analysis will focus on the providers operating websites with cooperative content, as those sites clearly illustrate the challenges brought about by the protection of freedom of speech and other rights in the Internet.

---

44 It is worth noting that the IPS category includes connection providers and service or content providers. This difference is quite clear, for instance, in the legal wording of Brazil's Internet Civil Framework, which establishes different levels of liability depending on the type of ISP involved. In this session, we will only deal with service providers and not with connection providers, as we understand that no filtering mechanism should be applied to the latter, except when it is necessary to comply with network management technical requirements.

Content filtering by service providers, when implemented pursuant to a court order, is often the consequence of actions for relief demanding a monetary award and the prohibition to continue exhibiting the content in the web.

In the case of collaborative sites, the content that appears on the webpage is not created by a central editing office, but rather by users themselves, who upload photographs, videos and music files or insert text. This content may have been created by the users and/or be owned by them, and should be adapted to comply with the terms of the content license for that particular website.

Nevertheless, when images, texts and music videos are created by others or when the copyright belongs to a third party —and use thereof is not contemplated by copyright exceptions and limitations—, the relevant authorization must be requested. Absent an authorization to disclose or in the event of other unauthorized uses of the work in question, without consideration of the users that disclosed unauthorized contents, the individuals or companies exploiting those collaborative websites, i.e. the Internet service providers, might be prosecuted for improper use of such content.

The same applies to other cases referred to in previous sections —involving content outside the scope of copyright which injures other people— regarding the possibility of holding service providers liable for statements made by their users showing prejudice based on gender, ethnicity, sexual orientation, etc.

In those legal actions, the author usually requests the judge to award damages and to prohibit the use of the materials that are the subject matter of the proceedings. That prohibition, imposed on the provider operating the website, normally determines that the penalty shall apply to every subsequent infringement of third party rights.

The problem with these court decisions is the filtering mechanism that providers should put in place to prevent the infringement of third party rights by their users. Such filter may be questionable in terms of efficacy and for the adverse effects that it may have on the technological, creative and innovative development of the network, especially as they might interfere with content that would not be the actual subject matter of legal actions and thus have an impact on network neutrality.

In the first place, it is necessary to raise some objections to content filtering mechanisms as a way to protect third party rights. Several complaints have been submitted to remove contents for alleged infringements, involving not only a violation of copyright, but also an infringement of image and privacy rights. On the other hand, that information may be deemed important for development purposes and hence be protected by the freedom of expression laws.

One of the first difficulties encountered in the discussion about filters is to identify the criteria to be applied when adopting a mechanism to select what may or may not appear on a website. Most court decisions establishing whether certain contents should be removed from a webpage only oblige the defendant to comply with the ruling, but fail to specify which terms should be used to put the filter in place, the sort of expression that should be prohibited, etc. There being no certainties regarding the methods to be applied to implement the filtering mechanisms, providers are authorized to establish their own criteria.

It is remarkable that, in this regard, the vagueness of court decisions could either benefit or jeopardize a defendant's position. This is because the mechanism to filter content protected by a certain regulation may be chosen freely, but at the same time the defendant may be subject to further actions if the filtering mechanism adopted fails to work as expected by the vague resolution; i.e. if the video, text, photograph or music piece at issue is uploaded again. In this second stage, the court will probably impose harsher penalties, as now the case will involve non-compliance with a court decision. What is not clear in court decisions is that, often, non-compliance results from the

technical difficulties of removing contents, especially in the case of collaborative websites. This difficulty is compounded by the lack of specificity of the judicial decision as to how the filtering process should be carried out.

While it is true that the defendant must always cooperate to minimize damage, if the defendant is left to decide how contents should be filtered, an excessive burden will be placed on the individual or company operating the site. They would be responsible for making complex decisions regarding online content viewing and for choosing the filtering mechanism, and they would even be exposed to further legal actions if the court holds that the action taken to mitigate the damage is inadequate. This is precisely the type of scenario that discourages innovation, and may also pave the way for abusive practices curtailing the right to freedom of expression and access to information. The worst of all is that it may not even help to realize the end pursued.

We may then hold that the lack of specificity regarding filtering criteria is a basic problem when this mechanism is analyzed as a potential barrier to technology development. However, there are at least three other aspects worth considering in connection with filter management, which may help understand the consequences of claims for damages. We may hold that court-ordered filtering (i) is ineffective; (ii) goes beyond the specific limits for which it was sought, and (iii) impairs network neutrality.[45]

Filtering devices are regarded as ineffective because, at the present state of technological development, it is impossible to guarantee with some degree of accuracy that certain content will not be available in collaborative websites. This is because the means used to circumvent filters are simple and are constantly updated. Hence, blocking specific materials becomes, in fact, a constant chase after new patterns to evade rules and control techniques.

In the case of collaborative websites that, following a judicial resolution, are required to put in place filtering mechanisms, without any indication as to methodology, the individual or company operating the website is charged with the obligation to create adequate conditions so that the content at issue is not uploaded again by the users of the site. Even though the prohibition may be established in the rules governing the use of the site, under the terms and conditions for use, they are actually rendered effective by means of a source code, i.e. the technological devices which have a strong impact on the effects of the regulation.[46] Even if there is an order requiring the removal of the complete website —as was the case in Brazil, when the Youtube site as a whole was banned for a few hours due to a complaint regarding image rights—, there are technological means which allow users to access those sites using, for instance, a proxy server,[47] circumventing filtering regulations.

Besides, it is important to underscore that the prohibition that stops certain websites from showing specific content does not prevent other sites from exhibiting them, even outside the scope of the country's jurisdiction. Therefore, the damage inflicted by the online presence of unwanted material is not eliminated. This is precisely the third test suggested by Lawrence Lessig in the decision issued in Napster's case: how effective would it be to file a claim for damages in order to suspend the activity of a file exchange network when the perfect filtering mechanism is not yet available? Users

---

[45] These three negative effects of filtering mechanisms have already been examined, from a different perspective, by Carlos Affonso Pereira de Souza, Pedro de Paranaguá Moniz and Sérgio Branco Vieira Júnior in "Neutralidade da rede, filtragem de conteúdo e interesse público: reflexões sobre o bloqueio do site Youtube no Brasil", in *Revista de Direito Administrativo*, issue no. 246 (September-December 2007); pages 67 et seq.

[46] See Lawrence Lessig, *Code and other Laws of Cyberspace*. Nueva York: Basic Books, 1999.

[47] Cf. "Brasil Telecom Censura a internet no Brasil bloqueando acesso ao YouTube," available at <http://www.softwarelivre.org/news/8219>, accessed on 08/15/2011.

would respond to such court decision by simply migrating to other websites, where the potential damage will continue.

In this connection, the lack of a network control center —which is very positive— prevents the adoption of filtering mechanisms that would cover all forms of online content viewing, and this makes it hard to impose liability and to realize the compensatory purpose. It is worth pointing out that such decentralization has lead to a level of cultural pluralism and freedom of expression that had never before been enjoyed in the mass media.

Tim Berners-Lee, considered one of the "fathers" of the Internet, when mentioning the perspectives that could be adopted to build its architecture, noted that:

"Among the market-oriented inspirations and the humanist ideals, we realized that adopting a control perspective would be a wrong decision. The network has been designed in such a way that there is not a single center where users must register their new servers or request authorization to upload new content. Anyone can create a new server or upload new content. In philosophical terms, if the Internet is to be a universal asset, it should be able to grow without restrictions. In technological terms, should there be a point of control, it would rapidly become a bottleneck for the growth of the Internet, which as a result would never reach the intended scale. Its most important trait was to be free from control."[48]

Therefore, we might conclude that claims for relief which are decided by orders requiring the implementation of content filtering mechanisms are, as a general rule, not very effective. Such solutions also have a negative impact on innovation and technological development through the Internet.

These effects are especially true when we realize that the filtering tends to go beyond the specific limits for which it was required, as the mechanisms implemented to comply with court orders often end up restricting access to other content in addition to that it was meant to prohibit.[49] For instance, if the filtering mechanisms are based on key words, other materials which were lawfully inserted in a cooperative website will probably be affected by those restrictions for using the same terminology. The same problem would affect works which have identical or very similar titles. This shows that filtering mechanisms need to be constantly improved to guarantee a minimum level of safety and to prevent a negative impact on third parties that have no connection whatsoever with the claim for relief at issue.

It is interesting to note, as a further proof of the awkward position in which Internet content providers find themselves, that anyone who feels impaired by the undue removal or filtering of content may bring an action to have their work featured on the web once again. Providers may try to avoid this kind of actions by including, in their terms and conditions, an explanation stating that the works exhibited may be subject to legal actions. However, that does not guarantee that the filtering mechanisms will not bring about other problems for the provider's business.

---

[48] Tim Bernes-Lee. *Weaving the Web: The original design and ultimate destiny of the World Wide Web by its inventor*. HarperCollins: New York, 1999; page 99. No mesmo sentido, enfatizando que a finalidade da Internet é criar um canal de difusão de informação cada vez amplo, sem qualquer escrutínio sobre a qualidade do que é transmitido por esse meio, vide Giuseppe Rossi. "Il cyberlaw tra metafore e regole", in Rivista di Diritto Civile, ano XLVIII, nº 06 (nov-dez/2002); p. 798.

[49] Tornou-se célebre na Internet o bloqueio de *websites* que relatavam a exploração espacial do planeta Marte por um carro-robô da NASA (National Aeronautics and Space Administration), pois a maior parte dos filtros inseridos em computadores domésticos para controlar a navegação de crianças impedia o acesso a *websites* que contivessem a palavra "sexo". Em inglês, juntando-se as palavras "Mars" (Marte) e "Exploration" (Exploração), o resultado é a palavra "sex", justamente bloqueada pelos sistemas de filtragem (http://query.nytimes.com/gst/fullpage.html?res=9D00E2D8163BF937A25756C0A9669C8B63, accessed on 15.08.2011).

In sum, our hypothetical scenario began with only one aggrieved party (the author of a piece of work that is available without the relevant authorization). Then there appeared a second aggrieved party whose problem resulted from the solution adopted to remedy the damage inflicted on the first party, i.e. by the filtering mechanism.

This scenario considerably reduces the chances for innovation on the Internet, as new providers may simply not adopt new business models for fear that they might be held liable for the actions of their users. As regards copyright infringements, if peer-to-peer network operators were held liable, this could discourage the development of such technology, which clearly has many uses other than the commission of crimes, as was established in the Betamax case.

In this respect, Casimiro de Vasconcelos Sofía points out that those technologies, "however, raise a number of seemingly insurmountable issues related to the fact that they tend to block more content that expected, and this could result in disguised censorship."[50]

In Brazil, the Court of Justice of the State of São Paulo had the chance to hear a case in which the company Anima Producciones Audiovisuales Ltda, owner of the copyright to the movie "Pelé Eterno," which portrays the footballer's life and career, filed a claim requesting the removal of the movie clips that were posted in YouTube. According to the case record, more than 100 video clips have been created by users, some including comments, new images, remixings or mash ups, etc. Those practices were considered unlawful uses of the intellectual work.[51] These are the most important paragraphs of the decision on "Agravo de Instrumento":

> "3. Regardless of the author's right to obtain any cash benefit from the use of its work, insisting on removing the content from the web, due to lack of authorization or assignment of rights, considering that an unauthorized reproduction has occurred, which consisted in defendants using third-party images, although other elements have been incorporated, the artistic unity of plaintiff is still evident and, for this reason, it is essential to grant the remedy. The requirements established in section 273 of the Code of Civil Procedure have been met, and the allegations and the evidence presented, as well as the well-founded fear of irreparable damage, have proved to be true.
>
> (...)
>
> 5. Based on the foregoing, protection is given in advance and the defendants are required to remove the content from their websites, under the penalty of paying a daily fine of $1,000.00. The pecuniary award shall not be applicable in the case of videos which are already available online, as blocking them would be technically impossible. Therefore, the defendants shall not be liable for the potential dissemination of such content through alternative "links" in other sites or portals, including the replacement of the video by third parties in the sites of the defendants, all of the above without prejudice to any award of damages that may be granted."

[50] Sofia de Vasconcelos Casimiro. *A Responsabilidade Civil pelo Conteúdo da Informação Transmitida pela Internet*. Coimbra: Almedina, 2000; p. 39.

[51] TJSP, Agravo de Instrumento n.o 497 958 4/7-00; rel. Des. Testa Marchi; j. em 13.03.2007.

This decision clearly shows the difficulties caused by the filtering mechanism and is cautious about imposing any liability for videos that may be accessed online[52] through alternative links[53] and which are impossible to block.

Finally, and reinforcing the negative effects of filtering mechanisms implemented as a result of legal actions, it may also be observed that such practices impair the neutrality of the web.

In the above-mentioned landmark case of the Brazilian model Daniela Cicarelli, in addition to removing the video from Youtube, the decision of the São Paulo Court of Justice, granting the author's petition, established that it was not possible to prevent the posting of the video and that, therefore, access to the defendants' websites should be suppressed within the national territory.[54]

This decision affected millions of Internet users in Brazil as it ordered the full suppression of the website. Although the new decision, published one day later, has made it clear that the court decision was not intended to block the website, two companies that operate the backbones of the Brazilian web actually blocked access to the website, to comply with what seemed to be the purpose of the court order.

Blocking an entire website because of one single video which allegedly infringed, in the case at issue, the image and privacy rights of two individuals, shows that filtering is a solution that impairs fundamental rights and does not serve the interests of the authors, since the implementation of filtering mechanisms fails to achieve a successfully balance between civil liability and the protection of fundamental rights in the worldwide web.[55]

In practice, in the claims for damages filed in Latin American courts, especially in Brazil, the aggrieved party often brings action against the service provider that hosts the content. As a result of this practice, the provider that operates a collaborative website is under constant threat of further legal actions. It is to be expected that, as a measure to prevent further legal action, service providers will enhance surveillance of content posted in the website by users.

However, this assumption has two major shortcomings. Initially, in order to monitor all the content posted on a collaborative website it would be necessary, depending on the size of the web page, to hire a large team charged with assessing the whole range of material hosted. The inclusion of automatic filtering mechanisms, as we have seen,

---

[52] Como a ação foi ingressada contra a empresa Google Brasil Internet Ltda, o pedido incluía, além da remoção de trechos do filme do *website* "You Tube", a sua eliminação também do *website* "Google Videos", ambos operados pela ré.

[53] Parece estar assentado na doutrina nacional e internacional que a pessoa que faz um *link* para determinada página não pode ser responsável pelo conteúdo que lá se encontra. Esse entendimento está baseado principalmente no fato de que o conteúdo da página direcionada pode ser alterado, sem que isso seja percebido pelo autor do *link*. A dinâmica de responsabilização por uma simples conduta como essa geraria não apenas um desestímulo para que fossem realizadas as conexões entre as páginas eletrônicas, que constitui uma das principais características da *world wide web*, como também exigiria um monitoramento não compatível com boa parte das atividades desempenhadas *online*. Nesse sentido, vide Flip Petillion e Sophie Huart. "La responsabilité des intermediaries dans la violation des droits d´auteurs", *in Droits Intellectuels: à la recontre d´une stratégie pour l´entreprise*. Brussels: Bruylant, 2002; pp. 577/579.

54 Cf. "Leia a íntegra da medida que manda desbloquear o YouTube no Brasil", available at <http://idgnow.uol.com.br/internet/2007/01/09/idgnoticia.2007-01-09.7954769479/IDGNoticia_view>, accessed on 08/18/2011.

55 Apenas como curiosidade, vale notar que no mesmo dia 09 de janeiro de 2007, data em que o TJ/SP esclareceu que não exigiu o bloqueio do YouTube inteiro, senadores norte-americanos trouxeram de volta à pauta a discussão sobre a neutralidade da web, por meio do *Internet Freedom Preservation Act* Cf. Gross, Grant: "Senadores dos EUA recolocam projeto sobre neutralidade na web em pauta", available at <http://idgnow.uol.com.br/internet/2007/01/10/idgnoticia.2007-01-10.8286737443/IDGNoticia_view>, accessed on 08/15/2011.

poses a series of problems that can only be corrected by human observation, but human surveillance may fail to assess the legality of a particular work.

Hiring specialized personnel and teams dedicated to reading and removing content from the website in advance will not be enough to mitigate the risk of potential legal actions. This is due to the fact that the criteria for assessing harmful material and the rights of third parties are not clear. In the absence of consistent criteria, the provider will probably choose to block the controversial content instead of maintaining it. Such a decision will not only impoverish the content in the website, but will also impose a sort of censorship that determines what may and what may not be accessible through the World Wide Web.

With regard to the unlikely situation in which the provider acts as an intermediary between users and the general public, from which a potential victim may arise, Ronaldo Lemos says:

> "Regarding the intermediary's liability in Brazil, it is surprising that, unlike other countries, no legal criteria have been established for releasing intermediaries from liability or for holding them liable upon notification. Therefore, Internet access providers work under conditions of uncertainty and fear regarding possible court decisions; as a result, they are more likely to remove the content without assessing the legitimacy of the request, since they do not have incentives to act otherwise. It should be noted that there is no "safe harbor" system in the country that can release the provider from liability by complying with certain requirements."[56]

The threat to innovation in the Internet posed by this scenario necessarily implies a deliberate reduction of content by providers who, fearing that they may have to face penalties, will choose to filter content that may eventually expose them to liability. As Ronaldo Lemos has pointed out, "a large part of the content in the web, though legitimate, has no legal protection at all… by threatening intermediaries, it is likely that content that is legitimate will be removed from the web without further consideration." [57]

In fact, those trends may create a dangerous vicious circle, which is contrary to the basic requirements of freedom of expression:

Judicial decisions ordering content removal barely specify the criteria used for filtering

Providers authorized to establish their own criteria

Risk of being challenged again in court if the action taken to stop damage is not effective enough (given the poor effectiveness of the filtering mechanisms currently in place)

ISP and Internet users exposed to legal insecurity

[56] Ronaldo Lemos. *Direito, Tecnologia e Cultura*. Rio de Janeiro: Editora FGV, 2005; page 125.

[57] Ronaldo Lemos. *Direito, Tecnologia e Cultura*. Rio de Janeiro: Editora FGV, 2005; page 125.

Tendency to adopt further filtering mechanisms without transparency

Source: prepared by the author

In fact, it would not be inaccurate to affirm that the future of innovation in the Internet is threatened by the adoption of filtering techniques and claims for damages. This scenario does not encourage new business models or innovation. The balance between the protection of legitimate rights (such as honor, copyright, etc.) and the freedom to engage in innovative activities that depend on technology and which may help guarantee other rights, such as citizenship and freedom of expression, is at risk. It is essential to bear this in mind at this particular stage of Internet regulation in Latin American countries, so as to guarantee the future of the Internet in the region, based on the principles of freedom, openness and network neutrality.

V. Conclusions

Internet content filtering is an issue that is difficult to grasp. While it is true that the application of those mechanisms implies a restriction on freedom of expression, at the same time there are a few legal excuses to justify filtering, such as child pornography cases. These reasons have been used to justify filtering practices that have extended to new cases reported and to new technology developed. Thus, in the face of excuses upholding copyright protection and the prevention of offenses against a person's honor, a series of mechanisms involving actual censorship become acceptable. These are widely rejected by the main international law treaties signed by the countries examined in this paper; however, they have been adopted by governments and companies intending to restrict the free flow of communication in the World Wide Web.

Even though most of the countries analyzed are not yet included in the international reports on countries that are "enemies" of freedom of expression in the Internet, the region has a track record of censorship on traditional press which has reflected, to a certain extent, on the web content. This potential must be at the core of our concerns as the region overcomes the digital gap and begins to regulate Internet practices.

In fact, the whole region is undergoing a special process, with all the countries establishing their Internet regulations, debating access policies, network neutrality laws and laws on intermediaries' liability. Regarding content regulation, the countries analyzed only incorporate specific provisions on filtering practices in their laws on child pornography. But in most of those countries, even though the remaining content regulations are not specifically applicable to the Internet sphere, they have been applied in the Internet environment. Therefore, it is worrying to note that certain crimes against a person's honor have been used to filter political content (mainly in Mexico, Venezuela and Colombia, but also in Brazil.) Other reasons for undue filtering are often related to violence or repression of copyright infringements.

This is the case, for example, of the actions for damages brought against service providers which were addressed in our analysis, especially the claims against providers offering social networks and search mechanisms. Brazil and Argentina[58] are good examples of a trend towards aggrieved parties filing complaints directly against the provider (often in cases of offenses to honor) requesting the removal of content, the application of filtering and monetary compensation. In Brazil, the widespread recognition of the Consumer Protection Code (Law No. 8078/90) by the courts favors

[58] http://www.google.com/transparencyreport/governmentrequests/AR/?p=2010-12 (accessed on 08/12/2011)

this scenario, as courts put the victims of this type of infringement on a level with consumers injured by defective products or services.

It is worth pointing out that most sections of this study dealt only with information on filtering cases derived from judicial proceedings. No data were available on cases of "voluntary" filtering, by either the government or private entities, before the content leads to a claim. The lack of such information causes even more concern if the aim is to guarantee that the Internet we access is in line with the principles of freedom of expression, openness and network neutrality.

Hence, no matter why a filtering mechanism is established, transparency is always vital in connection with the use of those mechanisms, and by transparency we mean letting the user know that content has been filtered and why. That is to say that if a service provider uses voluntary filtering mechanisms, it is important to inform the user about those mechanisms in the relevant terms of service. As for connection providers, they should not be authorized to filter any kind of specific content, but rather follow the principle of network neutrality in traffic administration, without consideration of any kind of specific content.

On the other hand, where a court order for content removal has been issued, it is important to inform the user seeking to access the site which included the removed content that such content has been blocked and the reasons for such measure. Such determination could at least make part of the court orders that, due to the judges' lack of technical knowledge, have resulted in excessive removals. To avoid this, the judge should bear in mind that, if certain content must be unavoidably blocked, such blockage should be clear and supported by objective reasons, under an appropriate definition of standards to minimize the discretion of the party that applies the filters and requiring transparency in those practices. This is to ensure that the implementation of the relevant orders does not go beyond the required blockage or filtering of specific content.

Ultimately, the discussion regarding whether a specific content in the web should be filtered is key to the future of the web and is also essential for the adoption of regulations that can ensure that its nature and architecture remain free and open. The debate about the decisions made and how they are applied helps us realize how complex this issue is and serves as a guide to understand and evaluate those options that have achieved significant progress towards the control of behavior and the prevention/compensation of damages resulting from content posted in the Internet, which entails a series of dangers.

Internet crimes, privacy, e-commerce and freedom of expression are only a few of the aspects involved in the debate over content filtering in the web. This broad range of issues reveals how the discussion on filtering mechanisms cuts across different fields of knowledge and affects the way in which we deal with different aspects of law enforcement facing technological advances.

Annexes – Comparison of law and case law in the countries examined

Internet Service Access

		Brazil	Venezuela				Colombia	Argentina	Chile	Mexico
Internet Access Right	Laws	Internet Civil Framework PEC 6/11 - Internet access as a constitutional right (Acceso a Internet como Direito Constitucional) Broadband National Plan (Plano Nacional de Banda Larga)	**Decree No. 825 of 2000.**	**Law on Social Responsibility in Radio, Television and Electronic Media ()**	**Constitution of the Bolivarian Republic of Venezuela**	**Organic Law on Tele-communications (Ley Orgánica de Telecomunicaciones)**	Law No. 1341/09. Bill No. 149/Senate	**Decree No. 554/97**	Constitutional Reform Project establishes Internet access right. More about the bill.	**Bill on Internet users' rights**
	Cases and case law									

		Brazil	**Venezuela**	Colombia	**Argentina**		Chile		**Mexico**
Network Neutrality	Laws	General Telecommunications Law (Lei Geral de Telecomunicações)	**Network neutrality in Venezuela**	National Development Plan (Plan Nacional de Desarrollo), section 56	**Bill No. S-1491/11**	**Bill No. 1159-D-2011**	Law No. 20453.	Network neutrality regulations	**About network neutrality in Mexico**
		Internet Civil Framework, sections 2, IV; 9 and 12.							**Telecommunications Law, (Ley de Telecomunicaciones) section 44.**
	Cases and case law								

Content Regulation

		Brazil	**Venezuela**	Colombia			**Argentina**		Chile		**Mexico**
Hate crimes	Laws	Racial Crimes Act, sections 1 and 20.	**Law on Social Responsibility in Radio, Television and Electronic Media (Ley de responsabilidad social en radio, televisión y medios electrónicos), section 28.**	National Constitution, Articles 11 et seq.	Criminal Code, sections 102, 144, 147, 201 et seq.	Intl. Convention on the Eradication of All Kinds of Racial Discrimination (Convención Internac. sobre la Eliminación de Todas las Formas de Discrimin. Racial.)	**Law No. 23592**	**Decree No. 1086/05**	Anti-Terrorism Act (Ley Antiterro-rismo)	Anti-Genocide Act (Ley de Ge-nocidio)	**Federal Law to Prevent and Eliminate Discrimination (Ley federal para prevenir y eliminar la discriminación)**
		Criminal Code, sections 140 to 141.									
		Law No. 8.072/90, section 2.									
		Brazil Constitution, Articles 5, XLII; 3, IV.									
		Law No. 2889/56, sections 1 and									**CRIMINAL CODE**

		3.										
	Cases and case law	Marcelo Valle Silveira Mello case. Mayara Petruso case.	**GOVERNMENT INVESTIGATES BLOG.**	**PUBLIC PROSEC. INVESTIGATES WEB SITE**	Nicolás Castro case.		Piedad Córdoba case.					

		Brazil			Venezuela		Colombia				Argentina	Chile		Mexico
Child porno-graphy; obscene and sexually explicit material	Laws	Children's Charter (Estatuto de la Niñez), sections 240 to 241-D.	Criminal Code, sections 227, 228, 230, 234 and 215.	Bill No. 494/08.	**Organic Law on the Protection of Children and Adolescents (Ley Orgánica de Protección al Niño, Niña y del Adolescente, LOPNA)**	**Law on the Protection of Children and Adolescents in Establish-ments for the Use of Internet, Videogame and other Multimedia Systems (Ley para la Protección del Niño y del Adolescente en Salas de Uso de Internet, Videojuegos y otros Multimed)**	Criminal Code, section 218.	Law No. 679 dated August 3, 2001 on Child Abuse and Pornography in Internet, sections 7, 8 and 10.	Law No. 1336 of 2009.	Optional Protocol to the Convention on Child Rights (Protocolo Facultativo de la Convención sobre los Derechos del Niño) on children trafficking, child prostitution and use of children in porno-graphy.	**Bill No. S-0256/11**	Law No. 19927	Bill Against Child Seduction in Virtual Media	**Criminal Code, section 202.**
												Bill for the amendment of the Criminal Code and the criminalization of child pornography in virtual media		

	Cases and case law	Operação carrossel	**A few years ago, an investigation was carried out in connection with pornographic videos involving adolescents that had been posted in YouTube. The information on the case was silenced after finding out that the videos had been posted by the teenagers involved.**	Paul Anthony Brailsford case.	In January 2011, Criminal Court No. 23 of Medellin Circuit Court sentenced Wilson Hernando Daza Duque to 10 years' imprisonment for a pornography crime involving minors. Investigators found out that Daza Duque, a music teacher aged 34, had created an account in social networks with the purpose of contacting minors. He then photographed those minors and threatened them with disclosing their pictures. When this crime was reported, the Investigation Technical Team of the Office of the Attorney General of Colombia searched the teacher's house and detained him. Even though Daza Duque pleaded guilty, his sentence was not reduced because the victims were minors.	

				We are not aware of the existence of any specific laws that prohibit obscene and sexually explicit materials on the Internet. Neither are we aware of any general rules on this matter that may be applicable to the Internet environment. Decision T-391-07 of the Constitutional Court analyzed the sexually explicit and coarse language used by a radio station and held that: "The authorities have the power, established by the Constitution, to put in place reasonable and adequate limitations on the social spreading of this kind of language, thereby protecting the rights of third parties. However, this does not mean that they are entitled to hamper their broadcasting through the mass media by censorship." We understand that, if the Constitutional Court maintains its current regarding case law, this criterion may be applied to obscene and sexually explicit contents on the Internet.	

		Brazil				Venezuela	Colombia				Argentina	Chile	Mexico
Intellectual property	Laws	Copyright Law, sections 7, XIII; 33; 41; 101-109.	Law on Software	Decree No. 1355/94	Brazil Constitution, Article 5, XXVII.	**Special Law on Information Technology Crimes (Ley Especial contra los delitos informáticos)**	Berne Convention.	Law No. 23 of 1982.	World Intellectual Property Organization (WIPO) Copyright Treaty.	WIPO Performances and Phonograms Treaty.		Reform of Intellectual Property Law	**Mexican Copyright Law (Ley de Derechos Autorales Mexicana)**
							National Constitution, Article 61 et seq.	Criminal Code, Title VIII.	Common Regime on Copyright and Related Rights (Régimen Común sobre Derechos de Autor y Derechos Conexos.)	Law No. 44 of 1993.			
	Cases and case law						Guillermo Veléz case						

		Brazil	Venezuela			Colombia		Argentina		Chile	Mexico
Slander and libel (defamation)	Laws	Criminal Code, sections 138-145. Election Code, sections 324, 325 and 326.	**The provisions on crimes against reputation contemplated in the Criminal Code could be applicable.**			Criminal Code, section 220 et seq.		**Law No. 26551**	**About Law No. 26551**	Criminal Code	**Civil Code.**
	Cases and case law		**Noticiero Digital case.**	**Jesús Majano case.**	**Cristian Fuentes case.**	Cláudia Lopez case.	Alfredo Molano case.				

		Brazil	Venezuela		Colombia		Argentina	Chile	Mexico
General prohibitions	Laws	Bill No. 84/99 - Cybercrimes	**General Banking Law (Ley General de Bancos.)**		Newsletter N.o 1 Legal Information and Communic-ation Technologies (Tecnologías de la Información y la Comunic., TIC.)	Habeas Data Law.	**BILL No. S-0209/09**		
	Cases and case law		**Parallel dollar case.**	**El Liberal Venezo-lano case**					**General laws on telecommunications in Mexico.**

Content Blocking, Content Removal, Filtering

		Brazil	Venezuela			Colombia	Argentina	Chile	Mexico
Service blocking based on 2.0 web	Laws								
	Cases and case law	Cicarelli Case	**ENGINEER ARRESTED FOR HIS TWITTER COMMENTS**	**CITIZENS ARRESTED FOR EXPRESSING THEIR OPINION ON TWITTER**	**MEDIA COMMISSION REQUESTS PROSECUTOR'S OFFICE TO INVESTIGATE INTERNET SOCIAL NETWORKS**				

		Brazil	Venezuela		Colombia	Argentina	Chile	Mexico
Web page blocking	Laws	Bill No. 7439/2010	**Law on Social Responsibility in Radio, Television and Electronic Media (Ley de responsabilidad social en radio, televisión y medios electrónicos.)**	**Law on the Protection of Children and Adolescents in Establishments for the Use of Internet, Videogame and other Multimedia Systems (Ley para la Protección del Niño y del Adolescente en Salas de Uso de Internet, Videojuegos y otros Multimedias.)**	The closing, blocking or limitation of the access to certain Internet sites may be ordered in two scenarios: for prevention purposes, in order to stop minors from accessing web pages that might affect their development and education, or at the request of subscribers or users. In cases of child pornography and related crimes, as these are illegal conducts, access blocking is the Internet service provider's obligation and is also a penalty that may be applied by the relevant authorities.	**Law No. 25690/02**		
			Law on the Protection of Children and Adolescents in Establishments for the Use of Internet, Videogame and other Multimedia Systems.		Resolution 1732 of 2007 issued by the Communications Regulatory Commission (Comisión de Regulación de Comunicaciones), sections 113 and 114.			
					Decree No. 1524 of 2002, section 6-5.			
					Law 679 of 2001, section 4.			

	Cases and case law	In general, the cases of content blocking are related to the protection of privacy, or to pain and suffering or property damages caused by contents posted on the Internet. We have no information on specific cases.	**The users of the ABA – CANTV (telecommunications company owned by the State of Venezuela) service often (at least one Friday per month) submit complaints because they cannot access certain websites. The most commonly affected sites are blogs hosted in Blogger or WordPress, and the websites Noticiero Digital (www.noticierodigital.com) and Chigüire Bipolar (www.elchiguirebipolar.net.) The government does not acknowledge the existence of any blocking mechanism.**	In November 2010, a webpage was closed by the judicial police. At that time, it was reported that a Colombian operation that investigated child pornography had authorized the closing of 5,000 webpages, after finding that photographs and videos were digitally downloaded using Internet connections. Another reported event was Teléfonica-Telecom's blocking of an Internet page known as rapidshare, with a traffic of 60,000 visits, based on "ethics policies and requirements by the Ministry of Information and Communications Technologies." Last, in 2010, the Constitutional Court ordered Dejusticia to remove the personal information and references of a girl from its website. In this case, the homosexual partner of the girl's mother wanted to adopt the girl, and the situation was being analyzed further to a guardianship suit in which our organization had initiated a citizen intervention action.			

		Brazil		Venezuela	Colombia	Argentina	Chile	Mexico
"Notice and Take Down"	Laws	Copyright Law, sections 102-110.	Bill No. 84/99. - Cybercrimes	**Law on Social Responsibility in Radio, Television and Electronic Media (Ley de responsabilidad social en radio, televisión y medios electrónicos.)**				
	Cases and case law				In Colombia, there are no specific legal provisions based on the principle of "notice and take down." There is, however, a general application of the "notice and take down" principle among technicians, based on the widespread practice in the US, and in case that a free trade agreement was signed with that country.			

		Brazil		Venezuela	Colombia	Argentina	Chile	Mexico
Reporting mechanisms	Laws	Private:	Public:	**Public: The Law on Social Responsibility in Radio, Television and Electronic Media (Ley de responsabilidad social en radio, televisión y medios electrónicos) and the National**	There is a series of steps to be followed to report, control and follow up Internet sites with child pornography content. The first step is to report complaints to the units specialized in sexual offences at the prosecutor's office. If the report is sustained, the usual proceedings are initiated at the Investigation Technical Team (Cuerpo Técnico de Investigación, CTI),			
		Safernet;	Federal Public Ministry- Anti-Cybercrime Group.					
		National Campaign	The Federal Public Ministry is					

		Against Pedophilia in the Internet.	governed by Law No. 75/93.	**Telecommunications Commission (Comisión Nacional de Comunicaciones, CONATEL.)**	the division of the prosecutor's office charged with the allocation of cases. The public prosecutor and the relevant commission are appointed to conduct the criminal investigation.			
	Cases and case law	Safernet admits reports on the following issues: child pornography, racism, advocacy or incitement of crimes against life, xenophobia, neo-Nazism, animal mistreatment, religious intolerance, homophobia and human trafficking. Reports for offensive content may be submitted with the Federal Public Ministry.			Internet Sano, a governmental project with cooperation from the private sector.			

		Brazil	Venezuela		Colombia	Argentina	Chile	Mexico
Libraries and Internet cafes	Laws		**Law on the Protection of Children and Adolescents in Establishments for the Use of Internet, Videogame and other Multimedia Systems (Ley para la Protección de Niños, Niñas y Adolescentes en Salas de Uso de Internet, Videojuegos y otros Multimedias), sections 8 and 10.**	**Law on the Prohibition of War Videogames and Toys (Ley para la Prohibición de Videojuegos y Juguetes Bélicos.)**	Law No. 1336 of 2009, s 4.			
	Cases and case law							**Data on Internet cafes in Mexico.**

Licenses and Liability

		Brazil		Venezuela	Colombia	Argentina	Chile	Mexico
ISPs' Liability	Laws	The ISP company may be created as any other legal entity. It must be clearly stated that one of the activities contemplated in the corporate purpose is the provision of access or information services on the web. Should the Internet access service be provided via radio or by means of ADSL technology, a license issued by the National Telecommunications Agency shall be required.	Internet Civil Frame-work.	**Law on Social Responsibility in Radio, Television and Electronic Media (Ley de responsabilidad social en radio, televisión y medios electrónicos.)**	Law No. 1341 of 2009, sections 10 and 15.			**Federal Telecommunications Law (Ley Federal de Telecomunicaciones.)**
	Cases and case law							

		Brazil		Venezuela	Colombia	Argentina	Chile	Mexico
Browser and content providers' liability	Laws	Internet Legal Framework (Marco Civil da Internet.)	Copyright Law (Lei de Direitos Autorais.)	**Law on Social Responsibility in Radio, Television and Electronic Media (Ley de responsabilidad social en radio, televisión y medios electrónicos.)**				
	Cases and case law							