Institute for Research on Internet and Society

Internet and jurisdiction

Blocking and network fragmentation mechanisms

IRIS
Instituto de Referência em Internet e Sociedade

Institute for Research on Internet and Society

Internet and jurisdiction

Blocking and network fragmentation mechanisms

Coordination
Fabrício Bertini Pasquot Polido
Lucas Costa dos Anjos

Authors
Laila Damascena Antunes
Matheus Rosa
Pedro Vilela

Graphic Project
André Oliveira e Lucca Falbo

Cover
Freepik

Layout
André Oliveira

Editorial Production
Instituto de Referência em Internet e Sociedade

Revision
Lucas Costa dos Anjos

Finalization
André Oliveira

SUMMARY

1. Initial Remarks[1]

The Westphalia model of the nation-state, based on territorial sovereignty, is directly distinguished from the internet model, which is based on descentralized, open, collaborative and filled with transborder movements - that also occur in cyberspace. Due to the fact that they have such diverse nature and characteristics, the connection between states and the internet is complex. The internet is structured especially by means of computer language (code) and physical infrastructure (computers, cables, satellites, among others). The state, on its turn, organizes and controls its territory and population through a constitution, laws, institutions and customs. Then, connecting geography and cyberspace is a complex task, in full construction and transformation nowadays[2]. One of the earliest internet visionaries and enthusiasts uttered in his manifesto of cyberspace independence:

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.[3]

Sovereign powers, however, enter the internet and go beyond their informational boundaries. There are several reasons why a State, a public or private entity, may want to relativize the cross-border and universal nature of the internet, especially by using technical mechanisms, knowledge and technologies for this purpose. As a technology originally designed to ignore the existence of national boundaries, the internet was responsible for a revolution in transnational communication, but it also had a number of legal consequences and diverse risks for users, governments and companies.

The difficulty in adjudicating transnational conflicts originated on the internet has caused governments and companies to seek to prevent the emergence of such disputes. Over the years, new technologies have enabled mechanisms to simulate and adulterate geographical boundaries, identifying or repositioning the origin of users in the global space, then restricting their full access to sites, content or services and thus reproducing in the internet environment the political divisions of the offline world.

Increasingly, the phenomenon known as “balkanization of the internet” concerns academics and civil society activists who fear that the fragmentation of the network will destroy their democratic and collaborative potential, a true catalyst for innovation and access to information.

This study first analyzes cases in which the transnational nature originating from the internet has been altered to meet political, cultural, economic and/or legal demands. Second, the technical mechanisms used by governments and companies to effect such

1 This research was coordinated by Professor Fabrício B. Pasquot Polido and Professor Lucas Costa dos Anjos, at the Institute for Research on Internet and Society - IRIS and the Study Group on Internet, Innovation and Intellectual Property - GNet, at Universidade Federal de Minas Gerais. Laila Damascena Antunes, Matheus Rosa and Pedro Vilela were the authors of this paper, which was translated into English by Lucas Anjos and Paloma Rocillo.

2 LESSIG, Lawrence. Code: Version 2.0. Nova Iorque: Basic Books, 2006. Available at: <https://goo.gl/kUcPRA>. Access on February 9, 2017.

3 BARLOW, John Perry. A Declaration of the Independence of Cyberspace. 1996. Available at: <https://goo.gl/kocxlM>. Access on February 9th, 2017.

fragmentation are briefly explained. Finally, we will discuss theories and principles regarding the transnational nature of the network, its impact on contemporary society and the possible consequences of its distortion. It should be emphasized that the fragmentation discussed here is of a technical nature, and the discussions about social and/or cultural fragmentation caused by the internet are not within the scope of this work.

2. Why is it called the balkanization of the internet?

The process of fragmentation of the internet by means of technical and legal mechanisms has been called "balkanization" of the internet. The term refers to the political fragmentation of Southern European states, on grounds of ethnic, religious and cultural differences, after the end of foreign rule over the region[4]. The phenomenon is characterized when governmental censorship programs, commercial interests, cybersecurity concerns and other dynamic changes in the internet ecosystem ultimately shatter the global network into several regional versions. This retaliation threatens universal communication, innovation, and economic prosperity brought about by the internet as it was initially structured.[5]

Network fragmentation is considered one of the greatest threats to the internet as we know it, and the importance of its universal character is recognized by several scholars[6] [7]. However, it seems doomed to become a reality, since governments and agents with high economic power implement technical measures that favor their interests. Differences in applicable law are also cited among the main reasons why governments adopt mechanisms of fragmentation of the internet. We will analyze some cases and contexts where different technical means were used to fragment the internet, creating idiosyncratic versions of the network in different jurisdictions.

a. The Great Firewall of China

The term "Great Firewall of China" originated in the 1990s and was coined to refer to a series of restrictive practices and regulations on the part of the Chinese government over the internet[8]. In order to control content, communication, and even to favor local endeavors, the Chinese government has sought, by means of a combination of different methods, to police content and connection providers, individual consumers, foreign websites and applications.[9]

The Chinese filtering system is mainly based on the filtering of a huge list of IP addresses considered inappropriate or sensitive by the government. The list is delivered

4 ALVES, Sergio, Jr. The Internet Balkanization Discourse Backfires, *SSRN Electronic Journal*. Disponível em: <https://goo.gl/pQpLF6>. Acesso em 17 de fevereiro de 2017. p. 1-2.

5 HILL, Jonah Force. A Balkanized Internet?: The Uncertain Future of Global Internet Standards. *Georgetown Journal of International Affairs*. 2012 p. 49-58.

6 CLARK, Liat, BERNERS-LEE, Tim. Wired. We need to re-decentralise the web. Disponível em: <https://goo.gl/txGONw>. Acesso em 10 de fevereiro de 2017.

7 MARKOFF, John. New York Times. Viewing Where the Internet Goes. Disponível em: <https://goo.gl/js8Gp4>. Acesso em 10 de fevereiro de 2017.

8 BARME, Jeremie e YE, Sange. Wired. *The Great Firewall of China*. Disponível em: <https://goo.gl/P5zF0l>. Acesso em 05 de fevereiro de 2017.

9 LEE, Jyh-An e LIU, Ching-Yi, Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China (March 7, 2012). *Minnesota Journal of Law, Science, and Technology,* Vol. 13, No. 1, 2012. Disponível em: <https://goo.gl/R6ZJ6Z>. Acesso em 05 de fevereiro de 2017. p. 127.

to backbone providers[10] [11], and specifically to China Telecom, who are then responsible for the backbone of the network infrastructure and the international connections of the Chinese internet. These providers are required to install specific devices that identify the source of data packets and discard them when originating from a vetoed address[12].

The list of vetoed content varies greatly, but there is a certain predominance of subjects of a political nature among those selected. Sites that host information associated with Taiwan and Tibet independence, human rights, the Falung Gong movement and other threats to the Communist Party, are often blocked[13]. Sites like The New York Times, the Economist, Amnesty International, BBC, among others, are usually blocked[14] [15]. The cases of information technology giants, such as Google and Facebook, are also widely studied. Due to the Chinese government's difficulties in regulating these companies, and also their resistance to act in the interests of the Chinese state, the Communist Party chose to completely restrict its access[16].

During its short stay in China, for example, Google was forced to remove search results related to the aforementioned content, such as the Tiananmen massacre and the Tibetan independence movement. Political pressures from both the Chinese and American governments, as well as the company's own policies, led the company to withdraw from the country and become permanently blocked[17].

The result is an internet in China considered fundamentally different from the rest of the world's: it is often compared to the ecosystem of a lagoon isolated from the rest of the ocean, where analogous Chinese versions replace applications accessed by users from the rest of the world[18].

b. Data location, Brazilian data centers the "Euro Cloud"

As opposed to the trend of free flow of cross-border data, there are data localization rules, which can be understood as "efforts at the national or regional level to regulate the flow of data across borders or to create incentives to localize data processing and storage".[19] Like the use of filtering mechanisms by the Chinese government, forced location of data has been pointed out as a threat to the integrity of the internet, which contributes to its balkanization. Restrictions on the location of data have already been proposed by a number of countries, notably Germany, Russia and Brazil, particularly

10 According to the Joint Release from the Ministry of Science and Technology and Ministry of Communications of May 1995: "The internet is organized in the form of backbones, or backbones, which are network structures capable of manipulating large volumes of information, basically consisting of traffic routers interconnected by high-speed circuits." COMITÊ GESTOR DA INTERNET NO BRASIL. Joint note from the Ministry of Science and Technology and Ministry of Communications (May 1995). Available at: <https://goo.gl/xlHXDB>. Access on March 3rd, 2017.

11 According to Marcel Leonardi: "The backbone, or" backbone, "represents the maximum level of hierarchy of a computer network. It consists of the physical structures through which it traps almost all of the data transmitted over the Internet, and is usually composed of multiple high-speed fiber-optic cables. " LEONARDI, Marcel. Responsabilidade civil dos provedores de serviços de internet. Op.cit.

12 FARIS, Robert, VILLENEUVE, Nart, Measuring Global Internet Filtering. In: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain (eds.), Access Denied: The Practice and Policy of Global Internet Filtering, Cambridge: MIT Press, 2008. p. 5-27

13 LEE e LIU,Forbidden City Enclosed by the Great Firewall, *Op. cit.* , p. 127

14 *Idem*. p. 131

15 For a complete list, access: <https://goo.gl/oYFhjc>.

16 LEE, Jyh-An, LIU, Ching-Yi, LI, Weiping, Searching for Internet Freedom in China: A Case Study on Google's China Experience. Cardozo Arts & Entertainment Law Journal, Vol. 31, No. 2, 2013. Available at: <https://goo.gl/oRGuKB>. Access on February 7, 2017, p. 409.

17 *Idem*. p. 416

18 MOZUR, Paul. Chinese Tech Firms Forced to Choose Market: Home or Everywhere Else, New York Times. Available at: <https://goo.gl/UMoEn8>. Access on February 10, 2017.

19 KUNER, Christopher. Data Nationalism and its Discontents. Emory Law Journal Online, v. 64, p. 2089, 2015. Available at: <https://goo.gl/VxMkfp>. Access on February 7, 2017

motivated by public pressures to combat cross-border cyber-surveillance and data espionage by foreign governments and transnational corporations.

These restrictions occur in the territorial scope and can be characterized in five major modalities: i. restriction of data processing by entities within a given jurisdiction; ii. requiring data to be stored "locally" (within a given territory); iii. changes in network architecture and use of data routing to keep them within a territorial space, as a kind of "information confinement"; iv. discriminatory policies that allow the implementation of these restrictions only by certain organizations, with the criterion of origin/nationality; and v. restrictions on the movement of certain categories of data across borders[20].

Notably, type (ii), local data storage, was widely debated during the elaboration of the Brazilian Internet Bill of Rights. The predictions regarding the implementation of data centers in the national territory did not advance neither were included in the final text[21]. However, this practice, by way of example, can be observed currently in Russia, with the recent LinkedIn block case being the most significant example of the consequences of Russian localization rules[22].

It is also noted that type v. restrictions on cross-border movement are applied within the framework of the European Union, from the models established by the former Directive 95/46/EC[23] and currently by means of Regulation 2016/679, also called General Data Protection Regulation[24]. It refers to the limitation of the transmission of data of European citizens to non-EU countries, except for those that offer a recognized level of adequate protection for the processing of personal data. A notorious example of an agreement deemed insufficient occurred in the Safe Harbor case, in a decision of the Court of Justice of the European Union of 2015, which invalidated the agreement allowing the transmission of data by / to companies in the United States.[25]

We will analyze two distinct cases in which the data location was discussed: the German proposal for a European cloud service and the attempt to include an obligation to locate data centers in the national territory in the Brazilian Internet Bill of Rights.

The German and Brazilian cases came as a reaction to Edward Snowden's revelations of the US government's mass surveillance programs, which included evidence that the National Security Agency spied directly on the private communications of Chancellor Angela Merkel and President Dilma Rousseff.[26] In response, the German government

20 See DRAKE, William J. and CERF, Vinton G. e KLEINWÄCHTER, Wolfgang. Internet Fragmentation: An Overview. Future of the Internet Initiative White Paper. World Economic Forum, p. 41, 2016. Available at: <https://goo.gl/wTlV1e>. Access on January 27, 2017.

21 BRAGA, Juliana. Governo não vai insistir em data center no país, diz Dilma no Facebook. G1 Globo.com, April 24, 2014. Available at: <https://goo.gl/PRMG69>. Access on February 7, 2017.

22 Rússia inicia bloqueio ao LinkedIn após decisão judicial. Folha de S. Paulo, 17 Nov 2016. Available at: <https://goo.gl/SDKPZX>. Access on February 7, 2017. In June 2016, the Russian parliament approved alterations to the Federal Law on Information, Information Technology and Information Protection of 2006, reaching exactly the access providers of content providers, considered as "communications service providers ("CSP") and" facilitators of information dissemination on the Internet "("FIDI"), under the terms of the law. In November 2017, the blocking of anonymous browsing tools and virtual private networks (VPNs). Ver LEXOLOGY, New Russian Legislation on Massive Telecoms Surveillance, July 12, 2016. Available at: <https://goo.gl/fHNZuV>, access on September 18, 2017.

23 EUROPEAN UNION. Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Diário Oficial da União Europeia, L 281, November 23, 1995, p. 31–50. Available at: <https://goo.gl/GKm9dD>. Access on February 7, 2017.

24 EUROPEAN UNION. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Diário Oficial da União Europeia, L 119, May 4, 2016, p. 1–88. Available at: <https://goo.gl/tzzWf8>. Access on February 7, 2017.

25 EUROPEAN COURT OF JUSTICE. Schrems v Data Protection Commissioner (C-362/14) (Request for a preliminary ruling from the High Court (Ireland)). Judgment of the Court (Grand Chamber), October 6, 2015. Digital reports (Court Reports - general). Available at: <https://goo.gl/bYDdaS>. Access on February 7, 2017..

26 MACASKILL, Ewan, DANCE, Gabriel. The Guardian. NSA Files: Decoded. 1 Nov 2013. Available at: <https://goo.gl/YoVhD1>.

promoted the NETMundial Conference in partnership with the Brazilian government, a new platform for debates on internet governance. The biggest effort, however, concerns the internet infrastructure development guidelines for the European Union proposed by Angela Merkel, in addition to the inclusion of a clause in the Brazilian Internet Bill of Rights that would require internet companies to treat data in Brazil to store them in data centers in the Brazilian territory. The creation of a new submarine cable connection between Brazil and Europe was also proposed and is under construction, so that traffic between regions does not have to pass through the United States.[27]

The legislative proposal regarding the installation of data centers in Brazil was abandoned after negative reactions from experts, who said that it was the ineffective and possibly harmful measure to the Internet in Brazil.[28] A presença da norma no projeto de lei do Marco Civil da Internet também era um dos maiores entraves a sua aprovação.

Such rule on the Brazilian Internet Bill of Rights was also one of the major obstacles to its adoption.

The German proposal involved the development of information infrastructure that would allow European citizens to opt for services that would store their data within the European Union and therefore be subject to the continent's privacy laws. German lawmakers saw the prominence of US companies in collecting and processing data as a threat to privacy protection for European citizens.[29] The proposal was colloquially called the 'Euro Cloud' and did not receive much attention later and, until the date of publication of this work, did not reach any significant progress.[30]

c. The "halal internet" and other cases of "national intranets"

Efforts by governments to create rigid barriers to the flow of information from abroad have become commonplace. One of the most notable cases is the initiative by the Iranian theocratic government to create the "halal internet". Halal is an Arabic word meaning "permissible"[31] and is generally used to refer to the diet allowed by the Koran. The term was then adopted to refer to the intranet composed only of content considered legitimate by the government of the Islamic Republic.[32]

The proposal works more like an intranet than an internet: a private network controlled by an organization. Intranets are common in corporate environments such as businesses or universities. Through various mechanisms, their managers can choose what type of content will be available. It is worth noting that the intranet has only a limited connection to the internet, or, in some cases, it has no contact with the worldwide computer network.

The Iranian case is notable because its justification is not based on purely legal issues: the Iranian government fears infiltration of Western culture through the internet.

Access on February 7, 2017.

27 RT News. Brazil-Europe undersea cable to hide web traffic from US Snooping. February 26, 2016. Available at: <https://goo.gl/05oopm>. Access on February 7, 2017.

28 BARABAS, Emily. CDT. Brazil's "Internet Bill of Rights" regains momentum in Congress. March 27, 2017. Disponível em: <https://goo.gl/ZwbjDJ>. Access on February 7, 2017.

29 The Register. 'European IT Airbus could lead to competition concerns'. Available at:: <https://goo.gl/3bKEqa>. Access on February 13, 2017.

30 BRANDON, Jonathan. Merkel, Kroes' proposition for EU Cloud "aren't contradictory" , says EC. Telecoms.com. February 17, 2014. Available at: <https://goo.gl/En5gVO>. Access on February 17, 2017.

31 'What is Halal'. Disponível em: <https://goo.gl/9cvdeR>. Acesso em 17 de fevereiro de 2017.

32 BEITER, Katie. 'Iran introduces Halal Internet'. The Medialine. Available at: <https://goo.gl/obxtVs>. Access on February 17, 2017.

Since the Islamic Revolution in 1979, the country has been positioned in an antagonistic way to the West and its institutions. The Iranian experience can inspire initiatives by other states that often experience cultural shocks catalyzed by the internet. Cultural differences, especially in relation to discourse issues, are among the main driving forces behind the fragmentation of the internet [33].

Other countries that have developed limited national content intranets and restricted internet access include Cuba,[34] Myanmar[35] and North Korea. In the latter state, the number of accessible websites is limited to 28,[36] most of which are restricted to government-friendly content.

3. Blocking mechanisms

In order to understand the possibility of implementing mechanisms for sharing the Internet space according to territorial borders, it is first of all essential to understand the basic functioning of the logical layer on which the internet is based.

The Internet, as we know it today, uses the TCP/IP[37] protocol to forward end-to-end data packets. All internet communication uses these packages, either to view a text page, to exchange instant messages or to perform a video conference.

In the network infrastructure, there is a specific type of computer called a router, whose job is to serve as a meeting point, or "node", of different connections (be they fiber optic cables, wireless networks or radio antennas), to direct correctly the packages that pass through it. The choice of encapsulating all packets under the same protocol (IP) is one of the Internet's greatest assets because it allows different networks in different structures to communicate freely.

Routers identify recipient computers and senders from their IP addresses, which are "stamped" on data packets. From there, they can properly conduct data traffic over the network. A common analogy is that it compares the routers of a network to mail and mail carriers and packets of data, to letters and packets. Couriers receive a letter or package from a sender and their mailers use the physical infrastructure of the city to get around and deliver the letter.

a. Content and access filtering

Content and access filtering is one of the main mechanisms adopted by access and content providers, whether by governmental requirement, whether by choice.

The purpose of using filtering mechanisms varies greatly according to the nature of the organization involved. Governments generally require the implementation of filtering mechanisms as a way to prevent unlawful acts or punishment of such acts. Companies do so as a way of observing norms of national law or as a way to avoid be-

33 CHANDER, Anupam, LE, Uyen, 'Data Nationalism'. Emory Law Journal, Vol. 64, No. 3, 2015. Available at: <https://goo.gl/vdZ5nC>. Access on February 17, 2017, p. 678-679.

34 PRESS, Larry, The state of the Internet in Cuba, 2011. Available at: <https://goo.gl/fQzQJj>. Access on February 17, 2017.

35 RHOADS, Christopher, FASSIHI, Farnaz. 'Iran vows to unplug Internet'. Wall Street Journal. 2011. Available at: <https://goo.gl/Za6UIq>. Access on February 17, 2017.

36 ASHER, Sara. 'What the North Korean Internet Really Look Like', BBC News. 2016. Available at: <https://goo.gl/ptc0c9>. Access on February 17, 2017.

37 Transmission Control Protocol/Internet Protocol.

ing called to respond in unexpected jurisdictions. Even users can choose to use filtering mechanisms for the purpose of escaping unwanted content or protecting their privacy.

The mechanisms used also vary greatly according to the technical or coercive capacity of the performer, as well as the minimum effectiveness required from them. Whatever the means of filtering chosen, they will hardly have full efficiency and a certain error rate will always be present, and may even lead to unexpected or unwanted side effects. Filtration may be overt or obvious to others.

It is also important to consider that any filtering must be accompanied by a precise database regarding the information, destination, origin or content that must be filtered. Building and maintaining this up-to-date database already requires a significant effort on its own, as the amount of information that will allow filtering can be vast (depending on the breadth of the filtering) and constantly changing. The filtering methods discussed here will take into account a defined cut of the resources required for filtering. Using the analogy of the postman so that it can prevent the sending or receiving of a letter, you will first need to know which addresses are blocked or which type of package should not be delivered.

Next, the main filtering or blocking mechanisms used today are explored[38].

b. Filtering by geographic location

Geolocation filters are used by content providers that want to restrict their site to a particular region. Typically, filtering occurs by country, and may, in more complex situations, filter by cities or areas within its territory. Currently, there are different geolocation technologies such as geo-identification - usually to add locations to photos and videos - and geoblocks - usually employed to block content in different locations. This study does not seek to analyze in depth the nuances of each of these technologies, but rather to understand the operation of location technologies and their impact on network fragmentation.

Choosing location criteria is often based on the best user experience, and the service or product is designed for your location. As a result, for example, the language in which the site is displayed changes, often by redirecting to a local site (e.g., www.google.com and www.google.com.br).

Because of geographic location filters, sites such as Netflix streaming, for example, offer different movie catalogs and series for each country. It's because of the filters that Spotify, Apple Music and Google Play Music can make specific songs available to users from different countries. Apps available from the App Store and the Play Store also vary by country where the internet connection is made.

Therefore, the best user experience is regularly used as a practice that also allows the filtering of content accessible to the user due to its geographical position, because some of the rights of the exhibition and audiovisual reproduction of these works vary territorially, according to the laws of each country. Content filtering can have several legal bases: intellectual property, consumer protection, defamation, censorship linked to special policies against hate speech, such as the dissemination of Nazism, among others.

38 Here, the terms filtering and blocking are used interchangeably in this work, such as in especialized published works on the subject.

Being in wide development in Law, it is important to emphasize that:

> [...] it is difficult to know whether norms will strengthen or weaken the regulatory influence of geo-location technologies. Society has not yet sufficiently clearly taken sides for there to be any clear norms in relation to their use. Nevertheless, it can perhaps be assumed that the majority of users will react negatively to discrimination based on location.[39]

However, initiatives can already be taken, notably the proposal for a regulation on "geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market"[40], the draft of which has been approved by the European Commission and by the Council of the European Union at the end of November 2016, for discussion in the European Parliament.[41]

As for the technologies themselves, there are so-called sophisticated and unsophisticated geolocation techniques. Sophisticated ones can be classified as of being the client's or the server's. A client-side geolocation technology is located on your computer or wireless device, often employing the Global Positioning System (GPS) or triangulation of nearby network towers. On the server side, the IP number is translated by a geographic location.[42] These technologies achieve a high degree of accuracy.[43]

Unsophisticated technologies, on the other hand, do not provide high accuracy, usually consisting of information exchanged between a computer and a website, or a server hosting the website. Examples of this information are the language, time/time zone, and location settings that may be required by certain systems.[44]

Because it depends on the application of other blocking mechanisms, geographic location filtering is not in itself a blocking tool, but a facilitator for blocking, usually of content, at different locations.

c. TCP/IP header filtering

A packet under the TCP/IP protocol consists of a header followed by the data it carries. This header contains the IP of the source and destination computers of that packet, i.e., who sent it and to whom it was sent.

In order to prevent certain content from being accessed, or data of any nature travel between two points, the router can be programmed to discard any packets coming from or intended for a given IP address. An IP-only lock will cause any service hosted at that address to become unavailable to the network.[45]

39 SVANTESSON, Dan Jerker B. Private International Law and the Internet. 3. ed. Holanda: Kluwer Law International, p. 543, 2016.
40 EUROPEAN UNION. Proposal for a Regulation of the European Parliament and of the Council on addressing geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC. Available at: <https://goo.gl/u9oh0a>. Access on February 12, 2017.
41 EUROPEAN COUNCIL. Geo-blocking: Council agrees to remove barriers to e-commerce. Available at: <https://goo.gl/FGv0jV>. Access on February 12, 2017.
42 Further on this paper IP filtering will be discussed in more detail.
43 SVANTESSON, Dan Jerker B. *Op.cit.*, p. 523-526.
44 Idem, p. 541-542.
45 MURDOCH, Steven, ANDERSON, Ross, Tools and Technology for Internet Filtering.. In: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds., Access Denied: The Practice and Policy of Global Internet Filtering, Cambridge: MIT Press, 2008. p. 59.

It is worth mentioning that a website may have multiple domain names, but will usually be hosted on only one IP address. Header filtering will block user access to all domain names assigned to that IP.

More precise filtering can be done by filtering the ports, which are also in the header. Ports differentiate services on the same IP and it is common for different types of applications to use specific ports. To block only web traffic, for example, you can block port 80, while port 25 is generally used for SMTP e-mail services.

Although we do not have access to the decisions that ordered the blocking of WhatsApp in Brazil, because they are kept confidential, it is probable that the method used by the access and backbone providers to prevent the use of the application by Brazilian users has involved some level of header filtering of TCP/IP.

TCP/IP filtering must be conducted through an access provider, which can result in unwanted side effects. A backbone provider is constantly acting internationally, and a decision that requires you to filter data packets from and/or to a certain number of IPs may have consequences for other jurisdictions. This was also the case of the WhatsApp blocking in Brazil, whose effects in 2015 were felt in several other Latin American countries, also served by a common provider.[46]

Once again using the postal mail analogy, header filtering is as if the postman were given a "blacklist" of blocked addresses and, at the time of delivery, discarded only letters and packages whose source or destination address were on that blacklist, disregarding what is inside a package or what is written in the letter.

Filtering by IP address can be bypassed by users with some technical knowledge through Private Virtual Networks (VPNs), which directly or indirectly act as an additional intermediary in the communication between user and site or blocked application. In the use of VPN, a user first connects to another network, usually foreign, to then connect to the desired site or application. The provider responsible for conducting the filtering will receive packets addressed to or originating from the IP address of the VPN and not from the site/application that it should block, thus being unable to know if the packet came or goes to one of the addresses that it should filter. The amount of VPNs available to the average user is enormous and its use is not illegal, therefore the addition of the IP of the VPN to the list of blocked addresses is disproportionate or even impracticable.

d. Packet content filtering

Blind filtering of any packet coming from or destined for a given address is generally considered an excessive measure. Situations where completely blocking the traffic of a website or an application are rare and usually disproportional in the fight against the illegal act that one wishes to sanction.[47]

A more precise sort of filtering is packet filtering. In addition to examining the header to find out where the packet came from and where the packet is going to, a network node can also inspect the contents of the packet and, from a pre-defined configuration of unwanted content, prevent its traffic. Content filtering requires more sophisticated infrastructure, since conventional routers are not originally programmed to

46 TUDO CELULAR. Argentina, Chile e outros países são afetados pelo bloqueio do WhatsApp. December 17, 2015. Available at: <https://goo.gl/XuFrgw>. Access on February 17, 2017.

47 MURDOCH, Steven, ANDERSON, Ross, Tools and Technology for Internet Filtering, Op. cit. p. 59.

perform this inspection.

One form of content filtering is known as Deep Packet Inspection and is used primarily by governments for surveillance and/or censorship of their citizens' activities, through their own infrastructure, or by using private security companies. The United States' National Security Agency (NSA), which became even more notorious after the revelations of Edward Snowden in 2013, makes use of deep packet inspection to analyze the content of all types of packets that travel through applications and providers in the United States[48]. Other governments, such as China, deliberately block certain packages based on their content for political and economic reasons: it is the so-called Great Firewall of China, which prevents typical content providers in the West, such as Google and Facebook, from being normally inaccessible in its territory[49].

Content filtering is severely criticized and is considered a violation of the right to privacy and of the principle of net neutrality. It is presumed that the secrecy of data packets traveling through the internet should not be violated.[50] The Brazilian Internet Bill of Rights prohibits deep packet inspection for the purpose of filtering content without prior judicial order in its article 7, sections III and IV.[51] The inspection of packages for content filtering also runs counter to principles of the decalogue of the Internet Steering Committee in Brazil, which, in its sections I and VI, stress the privacy of the user and the maintenance of net neutrality.[52] The Geneva Declaration of Principles of the World Summit on the Information Society also reiterates privacy in private communications as an important principle for internet governance, thus contributing to the rejection of package inspection in most cases.

Deep packet inspection and other types of content filtering are not always used for surveillance or censorship purposes. In some cases, they can be used more or less anonymously for legitimate traffic management and Quality of Service[53].

e. DNS rejection

Most Internet communications make use of the Domain Name System (DNS) rather than just IP addresses, especially common for web browsing. Therefore, one way to block access to certain sites or content is to intervene in the DNS system of the access providers.[54]

Simply put, when a user enters a URL on a website (e.g. www.google.com) in their browser, their computer first sends a question to their ISP's DNS server (or another one

48 DPACKET.ORG. Deep Security: DISA Beefs up security with Deep Packet Inspection of IP Transmissions. October 30, 2008. Available at: <https://goo.gl/WjoHYy>. Access on February 5, 2017.

49 EIGN, Ben e EINHORN, Bruce. The Great Firewall of China. Business Week. 12 Jan 2006. Available at: <https://goo.gl/uoD194>. Access on February 5, 2017.

50 FUCHS, Cristian. Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society. The Privacy & Security Research Paper Series, Issue # 1 Uppsala, Centre for Science, Society & Citizenship. 2013.

51 Chapter II - Users' Rights and Guarantees. Art. 7. Internet access is essential for the exercise of citizenship rights and duties, and users have the right to: III – confidentiality of stored private communications, which may only be disclosed by judicial order; IV – maintenance of Internet connection, unless it is terminated due to the user's failure to pay for its use; BRASIL. Lei nª 12965, 23 de Abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Available at: <https://goo.gl/t93wcy>. Access on February 5, 2017.

52 The decalogue of the Internet Steering Committee in Brazil states that: "The use of the Internet should be guided by the principles of freedom of expression, individual privacy and respect for human rights, recognizing them as fundamental for the preservation of a just and democratic society. Traffic privileges should only respect technical and ethical criteria and political, commercial, religious, cultural, or any other form of discrimination or favoritism should not be allowed".

53 Quality of service will be further explained in section IV of this study.

54 MURDOCH, Steven, ANDERSON, Ross, Tools and Technology for Internet Filtering, Op. cit. p. 61.

the user has manually configured) . The DNS server then checks the IP number associated with that URL and returns it to the user, who can communicate directly with the site or application through the IP number.

Thus, it is possible for the access provider to filter users' browsing at this resolution stage, returning the user an invalid IP number each time certain URLs are requested. This form of filtering is relatively easy to fool, since the user can set up his or her computer to access a DNS server different from the default one used by the provider to return to normal browsing. The Google DNS server, for example, is widely used.

One of the judgments with the greatest repercussion worldwide in regard to DNS filtering mechanism is undoubtedly the case of LICRA v. Yahoo!, 2000[55]. With the ruling of a French court, Yahoo! was prohibited from announcing auctions of Nazi memorabilia products, as such practice is prohibited by law in France, despite the claim that such auctions would occur in the jurisdiction of the United States of America, since the servers were in US territory. However, the auctions were open to participants from any country.

Another claim sustained by Yahoo! argued for the technical incapacity to comply with the blocking order, to which the French court responded with the convening of experts to give their opinion on the most appropriate mechanisms. The method indicated was the blocking by DNS, which would allow to identify the French users. Instead of filing an appeal in France, Yahoo! Inc. filed a lawsuit in the United States arguing that the French court's decision was not valid in the United States for violating the First Amendment of the Constitution, which guarantees the right to freedom of expression. In a higher-court ruling, not reversed by the Supreme Court, the United States did not establish jurisdiction over the French parties, and the case had a strong rebuttal against Yahoo!.

Another case of significant importance occurred in October 2016, when a Distributed Denial of Service (DDoS) attack hit the US company Dyn, impacting the DNS system. As a result, millions of people lost access to various websites such as Twitter, Spotify, Netflix and PayPal, as the company's system has been overwhelmed by access requests.[56] It is unclear who and what motivated the attack, but there remains the attack on a basilar internet service by the DNS provider.

4. Net neutrality

In relation to internet governance, an important topic is always present in the discussions: net neutrality. It is a principle that emerged in the beginning of the 21st century, and has as one of its main theorists the American academic Tim Wu, a professor at Columbia Law School. According to The Net Neutrality Compendium:

> Network neutrality prescribes that Internet traffic shall be treated in a non-discriminatory fashion so that Internet users can freely choose online content, applications, services and devices without being influenced by discriminatory delivery of Internet traffic[57].

55 FRANCE. Tribunal de grande instance. Ligue contre le racisme et l'antisémitisme et Union des étudiants juifs de France c. Yahoo! Inc. et Société Yahoo! France (LICRA v. Yahoo!).

56 This case also demonstrated the security flaws currently exploitable in the so-called "internet of things", which integrates objects such as doors, clocks, coffee machines, etc. into the network. See HILTON, Scott. Dyn Analysis Summary Of Friday October 21 Attack. Available at: <https://goo.gl/jpUjkS>. Access on February 9, 2017.

57 BELLI, Luca; FILIPPI, Primavera De. The Net Neutrality Compendium: Human Rights, Free Competition and the Future of the Internet. P. 3. 1st ed. Suíça: Springer, 2016.

According to advocates of net neutrality, this principle is responsible for maintaining an open architecture network on the internet, where users can consume, produce and share all kinds of content between them. Net neutrality thus preserves the very integrity of the internet.

There are at least three ways to discriminate a content or application on the internet: blocking, slowing down or charging different access prices. To illustrate this situation, imagine a country that does not protect net neutrality. In it, access providers are allowed to provide internet plans with access to specific sites, similar to what happens on cable TV nowadays, where users buy packages with access only to sports, movie, cooking or news channels, for example. An access provider could offer a cheaper internet package with access to the top sites in the world. But start-up internet sites, startups, or content related to culture dissemination could be in a more expensive package, which would hurt young companies, as well as prevent access to education. In addition, in that country, the government would have the authority to block any content that it deemed undesirable for the access of its population.

There are those who argue that neutrality is harmful to the consumer and the internet. They argue that net neutrality prevents consumers from choosing and purchasing access only to sites they actually want, and are forced to pay for access to content types that they rarely, if ever, consume. In addition, those who oppose network neutrality argue that this principle harms the internet, as the global computer network lacks the structure to provide unlimited access to its 3 billion users. If there is no content discrimination, it may, in the near future, collapse.

Due to the controversies intrinsic to the theme, net neutrality is the subject of frequent debates in countries that seek to legalize it. Latin American countries are considered a reference in terms of internet governance and protection of the principle of net neutrality. Brazil (Brazilian Internet Bill of Rights - Law 12.965)[58], Chile (General Telecommunications Law - Law 18,168)[59] and Argentina (Argentine Digital Law - Law 27,078)[60] were pioneers in protecting this principle.

In the United States, net neutrality is the subject of frequent debates among large internet-connected corporations and civil society sectors. The Federal Communications Commission (FCC) is in favor of network neutrality, having approved, in February 2015, The FCC's Open Internet Rules, i.e. The FCC Rules for Open Internet. This regulation presents important provisions, preventing the blocking, discrimination and prioritization of content.

According to The FCC's Open Internet Rules, access providers can not block ac-

58 "Art. 3. The following principles underlie Internet governance in Brazil: [...] IV – preserving and guaranteeing network neutrality;" BRASIL. Lei 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Available at: <https://goo.gl/C7KI9J>. Access on February 6, 2017.

59 "Artículo 24 I.- Para la protección de los derechos de los usuarios de Internet, el Ministerio, por medio de la Subsecretaria, sancionará las infracciones a las obligaciones legales o reglamentarias asociadas a la implementación, operación y funcionamiento de la neutralidad de red que impidan, dificulten o de cualquier forma amenacen su desarrollo o el legítimo ejercicio de los derechos que de ella derivan, en que incurran tanto los concesionarios de servicio público de telecomunicaciones que presten servicio a proveedores de acceso a Internet como también éstos últimos, de conformidad a lo dispuesto en el procedimiento contemplado en el artículo 28 bis de la Ley N° 18.168, General de Telecomunicaciones." CHILE. Ley 18.168. Ley General de Telecomunicaciones. Available at: <https://goo.gl/ZaDRFY>. Access on February 6, 2017.

60 "ARTÍCULO 56. — Neutralidad de red. Se garantiza a cada usuario el derecho a acceder, utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación, servicio o protocolo a través de Internet sin ningún tipo de restricción, discriminación, distinción, bloqueo, interferencia, entorpecimiento o degradación."ARGENTINA. Ley 27.078. Ley Argentina Digital. Available at: <https://goo.gl/qGzigf>. Access on February 10, 2017.

cess to legal content, applications, services or devices that are not considered harmful. Access providers may not harm or degrade legal internet traffic based on non-harmful content, applications, services, or devices. And broadband providers can not favor some licit internet traffic over other legal traffic in return for any consideration. However, the US Congress has not yet legislated on the issue, making The FCC's Open Internet Rules ineffective.[61]

In Europe, in 2015, the European Parliament adopted Regulation (EU) 2015/2120, laying down measures concerning open internet access[62]. In its section I:

> This Regulation aims to establish common rules to safeguard equal and non-discriminatory treatment of traffic in the provision of internet access services and related end-users' rights. It aims to protect end-users and simultaneously to guarantee the continued functioning of the internet ecosystem as an engine of innovation. Reforms in the field of roaming should give end-users the confidence to stay connected when they travel within the Union, and should, over time, become a driver of convergent pricing and other conditions in the Union[63].

On August 30, 2016, the Body of European Regulators for Electronic Communications (BEREC)[64] published the Guidelines for National Regulatory Authorities (NRAs)[65], a directive[66] that establishes rules to be followed to implement network neutrality in the continent. The Directive imposes strict restrictions on the practice of zero-rating, and prohibits traffic management, except when there is a need for quality of service[67]

Whether or not in favor of this concept, the importance of net neutrality as a tool in the struggle for the maintenance of the integrity of the internet is undeniable. If this principle is respected, the State and access providers will not be able to discriminate content based on political and/or economic criteria.

In order to understand the impact of programs and applications in the context of internet fragmentation, taking into account the principle of net neutrality, the analyzes of the Free Basics application and practices known as zero-rating and quality of service are fundamental.

61 FEDERAL COMMUNICATIONS COMMISSION. *Open Internet.* Disponível em: <https://goo.gl/sRHoNZ>. Acesso em 06 de fevereiro de 2017.

62 Parlamento Europeu aprova neutralidade da rede e extingue roaming entre países do bloco. O Globo, Amsterdã, April 3, 2014. Available at: <https://goo.gl/KZOSQD>. Access on February 10, 2017.

63 EUROPEAN UNION. Regulamento (UE) 2015/2120 do Parlamento Europeu e do Conselho de 25 de novembro de 2015 que estabelece medidas respeitantes ao acesso à Internet aberta e que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas e o Regulamento (UE) nº 531/2012 relativo à itinerância nas redes de comunicações móveis públicas da União. P. 1. Jornal Oficial da União Europeia L 310/1, November 26, 2015. Available at: <https://goo.gl/xloHrF>. Access on February 10, 2017.

64 BEREC is a European Union (EU) agency providing administrative and professional support services to the Body of European Regulators for Electronic Communications. BEREC shall ensure the uniform application of relevant EU legislation in order to ensure the correct functioning of the single market for electronic communications in the EU. EUROPEAN UNION. Gabinete do Organismo de Reguladores Europeus das Comunicações Eletrónicas. Available at: <https://goo.gl/KHwM0p>. Access on February 10, 2017.

65 BEREC. Comunicado de imprensa: O BEREC publica Linhas de Orientação sobre neutralidade de rede (net neutrality), August 30, 2016. Available at: <https://goo.gl/gPL2bb>. Access on February 10, 2017.

66 A 'directive' is a legislative act setting out a general objective that all EU countries must achieve. However, it is up to each country to draft its own legislation to comply with this objective. EUROPEAN UNION. Regulamentos, diretivas e outros atos legislativos. Available at: <https://goo.gl/WEfbXI>. Access on February 10, 2017.

67 BEREC. BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules. Available at: <https://goo.gl/jwjwhI>. Access on February 10, 2017.

a. Free Basics

Free Basics, initially called Internet.org, is a project developed by the social network Facebook in partnership with companies Samsung, Ericsson, MediaTek, Opera Software, Nokia and Qualcomm, which emerged in the year 2013. According to the site:

> Free Basics by Facebook gives people access to useful services on their cell phones in markets where Internet access may be more expensive. The sites are available for free without charge and include content such as news, jobs, health, education and local information. By presenting people with the benefits of the Internet through these sites, we hope to include more people online and help improve their lives.[68]

This project was developed with the goal of providing free internet access for the most needy populations on the planet. To do this, in addition to the usual infrastructure required to access the worldwide computer network (for example, fiber optics), drones are also being used to reach the most inaccessible regions.[69] To use the internet through the program, it is critical that users have a device with wi-fi to download the Free Basics application. This application has a web browser, with access to sites selected by Facebook and partner companies.

The way Free Basics works has polarized discussions between academics, civil society, and government. Those who disagree with the program claim that it seriously undermines the principle of net neutrality, since it provides access only to previously selected sites, thus fragmenting the virtual space. In addition, Free Basics could either alienate new users, as they would have a "partial" view of the internet, as well as use users' data unlimitedly. However, those who agree with the program argue that it shows concern for marginalized sectors of society, as people in misery could only access the internet through Free Basics. In addition, its advocates claim that the program works as an incentive, demonstrating the benefits of the internet for those who are not included in the virtual environment.

To date, Free Basics is present in more than fifty-three countries, divided between Africa, Latin America (Facebook plans to bring to Brazil in the near future[70]), Asia and the Middle East. However, governments in India[71] and Egypt,[72] which initially allowed the application in their territories, banned the use of it in the year 2016.

b. Zero-rating

The zero-rating practice can also be considered a threat to the integrity of the internet. According to BEREC:

68 Free Basics by Facebook. Available at: <https://goo.gl/bcPVMz>. Access on February 10, 2017

69 Mark Zuckerberg anuncia drones para Free Basics. *Soluciones Telcel*, February 26, 2016. Available at: <https://goo.gl/QOJ08j>. Access on February 10, 2017.

70 Facebook está preparando lançamento do Free Basics no Brasil. Canaltech, April 14, 2016. Available at: <https://goo.gl/vRT9ff>. Access on February 10, 2017.

71 GARATTONI, B. Índia proíbe novo serviço do Facebook; veja por que. Super Interessante, February 22, 2016. Available at: <https://goo.gl/gJwDKY>. Access on February 10, 2017.

72 Programa de internet gratuito é proibido no Egito. O Globo, Cairo, December 30, 2015. Available at: <https://goo.gl/xSBTrB>. Access on February 10, 2017.

> Zero-rating' is when an ISP applies a price of zero to the data traffic associated with a particular application or class of applications (and the data does not count towards any data cap in place on the internet access service)[73].

To illustrate this practice, imagine an internet service provider providing free access to the WhatsApp messaging application, but charging for access to similar competing applications such as Telegram or WeChat. This situation, in addition to representing unfair competition, also fragments the internet, by inducing the user to use certain application only by not charging the users' credits.

In Latin America, Brazil, Argentina and Chile stand out in the fight to curb zero-rating. In Brazil, Decree No. 8,771, in Articles 9 and 10, contains provisions expressly prohibiting this practice[74]. Argentina (Argentine Digital Law)[75] and Chile (General Telecommunications Law)[76] indirectly prohibit zero-rating.

In addition to Latin American countries, India and Europe have been working to ban the zero-rating. The Asian country has banned tariff discrimination based on content accessed by users through the Telecom Regulatory Authority of India[77]. On the European continent, BEREC presented directives restricting the zero-rating practice in its guidelines issued in 2016[78]. However, the document allows for different interpretations to argue that there are different types of zero-rating, and the national authorities should assess whether it even harms the consumer and the innovation ecosystem of the internet.[79]

Finally, it should be noted that zero-rating must not be confused with quality of

73 BEREC. What is zero-rating? Available at: <https://goo.gl/4MAvqd>. Access on February 13, 2017.

74 Free translation by the author: "Article 9 - Unilateral conduct or agreements between the person responsible for transmission, switching or routing and application providers are prohibited, which: I - compromise the public and unrestricted character of Internet access and the principles, principles and objectives of the use the Internet in Brazil; II - prioritize data packets due to commercial arrangements; or III - privilege applications offered by the person responsible for transmission, switching or routing or by companies that are part of their economic group. Article 10. Commercial offers and charging models for internet access should preserve a single internet, of an open, plural and diverse nature, understood as a means to promote human, economic, social and cultural development, contributing to the building an inclusive and non-discriminatory society". BRASIL. Decreto Nº 8.771, de 11 de maio de 2016. Regulamenta a Lei no 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Available at: <https://goo.gl/5Dikve>. Access on February 13, 2017.

75 "ARTÍCULO 57. - Neutralidad de red. Prohibiciones. Los prestadores de Servicios de TIC no podrán: a) Bloquear, interferir, discriminar, entorpecer, degradar o restringir la utilización, envío, recepción, ofrecimiento o acceso a cualquier contenido, aplicación, servicio o protocolo salvo orden judicial o expresa solicitud del usuario." ARGENTINA. Ley 27.078. Ley Argentina Digital. Available at: <https://goo.gl/qGzigf>. Access on February 10, 2017.

76 "Artículo 24 H.- Las concesionarias de servicio público de telecomunicaciones que presten servicio a los proveedores de acceso a Internet y también estos últimos; entendiéndose por tales, toda persona natural o jurídica que preste servicios comerciales de conectividad entre los usuarios o sus redes e Internet: a) No podrán arbitrariamente bloquear, interferir, discriminar, entorpecer ni restringir el derecho de cualquier usuario de Internet para utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio legal a través de Internet, así como cualquier otro tipo de actividad o uso legal realizado a través de la red. En este sentido, deberán ofrecer a cada usuario un servicio de acceso a Internet o de conectividad al proveedor de acceso a Internet, según corresponda, que no distinga arbitrariamente contenidos, aplicaciones o servicios, basados en la fuente de origen o propiedad de éstos, habida cuenta de las distintas configuraciones de la conexión a Internet según el contrato vigente con los usuarios". CHILE. Ley 18.168. Ley General de Telecomunicaciones. Available at: <https://goo.gl/ZaDRFY>. Access on February 6, 2017.

77 SANTOS, Vinicius W.O. Como a Índia baniu o zero rating. Observatório da Internet no Brasil, February 11, 2016. Available at: <https://goo.gl/Go1wBE>. Access on February 13, 2017.

78 "41. A zero-rating offer where all applications are blocked (or slowed down) once the data cap is reached except for the zero-rated application(s) would infringe Article 3(3) first (and third) subparagraph (see paragraph 55)". BEREC. BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules. P. 11. Available at: <https://goo.gl/jwjwhI>. Access on February 10, 2017.

79 BEREC. BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules. p. 11-12. Available at: <https://goo.gl/jwjwhI>. Access on February 10, 2017.

service. The first one concerns tariff discrimination between similar applications, while the latter concerns data discrimination between applications of different classes.

c. Quality of service

Quality of service is a form of data discrimination used by access providers. The quality of service discriminates data from packages with different contents in order to benefit the best internet operation for the user.

Imagine the hypothesis that a user is watching a movie on Netflix on their Smart TV, and another user, from the same household (and even IP), is sending e-mail using their cell phone. Considering this situation, the film should have a priority over the email, because a ten or twelve-second delay in receiving this is not bad for the user, since an email is not a message of urgency. However, a ten or twelve-second delay in playing the movie is something that will surely frustrate the user.

Access providers prioritize movie data for the benefit of e-mail data, so there is a higher quality service. This practice is not considered bad, since it maintains the good functioning of the internet.

In Brazil, the Brazilian Internet Bill of Rights (Law n. 12,965)[80] eand Decree No. 8,771[81] were concerned not to prohibit quality of service. It is important to point out that Brazilian law regards quality of service as an exception practice, that is, for exceptional situations where there is heavy traffic on the network. However, the tendency for the future is that this practice be used more frequently, since 50% of Brazilian households already have access to the internet[82]. With more users integrated with the world computer network in the country, practices that optimize navigation are essential, as well as improvements in the physical structure of the internet.

5. Internet and States

AJust as there is no global government, there is no such thing as an international internet tribunal dedicated to resolving disputes arising out of the network or a convention determining internet governance. The peaceful settlement of disputes that are of a nature in Internet relations presents major challenges for States. In search of solutions, alternative methods of conflict resolution or out-of-court mechanisms are often employed.[83] When the Judicial Power is activated, it is noticed that new rules are created,

80 Art. 9. The agent in charge of transmission, switching, and routing must give all data packets equal treatment, regardless of content, origin and destination, service, terminal or application. §1. Traffic discrimination and degradation will be subject to regulations issued under the exclusive powers granted to the President of the Republic in article 84 (iv) of the Federal Constitution, for the better implementation of this Law, after hearing the Brazilian Internet Steering Committee (CGI.br) and the National Telecommunications Agency (Anatel), and may only result from: I – technical requirements essential to the adequate provision of services and applications. BRASIL. Lei 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Available at: <https://goo.gl/C7KI9J>. Access on February 16, 2017.

81 Art. 4o A discriminação ou a degradação de tráfego são medidas excepcionais, na medida em que somente poderão decorrer de requisitos técnicos indispensáveis à prestação adequada de serviços e aplicações ou da priorização de serviços de emergência, sendo necessário o cumprimento de todos os requisitos dispostos no art. 9º, § 2º, da Lei nº 12.965, de 2014. BRASIL. Decreto Nº 8.771, de 11 de maio de 2016. Regulamenta a Lei no 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Available at: <https://goo.gl/5Dikve>. Access on February 16, 2017.

82 GOMES, Helton Simões. Internet chega pela 1ª vez a mais de 50% das casas no Brasil, mostra IBGE. G1, São Paulo, April 6, 2016. Available at: <https://goo.gl/SZZpcJ>. Access on February 16, 2017.

83 BYGRAVE, Lee A. e MICHAELSEN, Terje. Governors of internet. In: BYGRAVE, L. A.; BING, J. (eds.). Internet Governance: Infrastructure and Institutions. Oxford: Oxford University Press, 2009, p. 92–93.

special to the online context. Even so, it is also common to reformulate standards that, although precedent to the new technologies, can be transplanted if they are found to be adequate - generally, these norms deal with legal situations that exist in both offline and online worlds, such as eg Contract of purchase and sale.

Moreover, one of the main characteristics of the Internet is its interoperability, namely the structural functions that allow the connectivity and operability of different networks and devices. This characteristic, however, can not be considered as resulting from the efforts of States. Although countries indeed establish rules and principles for regulating the Internet, interoperability is a structural and fundamental aspect of functionality on the internet. Anywhere in the world, protocols such as TCP / IP or standards such as HTML, for example, work the same way, ensuring interconnectivity and standardization for users and maintainers of the network. The absence of interoperability, therefore, leads to the absence of interconnectivity, which in turn affects the ability to create connections of various types - connections that are responsible for making the internet work as such.

The notion of legal interoperability emerges as a possible means to solve network conflicts and harmonize legal regimes in different national territories, thus avoiding further fragmentation of the internet. The term has a recent origin in the face of the expansion of the internet and the challenges it imposes on legal systems. However, it represents an old idea: cooperation between different jurisdictions, making legal rules more harmonious in order to facilitate global communication, promote innovation and reduce costs in cross-border operations.[84]

In the procedural framework, legal interoperability can be developed through the use of multi-stakeholder participation and increased public transparency. Another way of achieving interoperability is through Private International Law, which stipulates rules on conflicts of laws - that is, the law applicable to the particular case. However, the rules provided by private international law do not indicate the answer to the case - the solution sought by the parties - but only point to the applicable law, which is therefore an indirect influence on legal interoperability.[85]

As regards the material scope, we can cite Directive 2000/31 / EC, which deals with electronic commerce in the European digital single market.[86] Another example of a document harmonizing substantive rules is the Convention on Cybercrime, also known as the Budapest Convention, of the Council of Europe.[87] In the rest of the world, legal interoperability still incipient in the internet, but it is possible to mention the International Telecommunication Union (ITU), the Internet Engineering Task Force and the World Wide Web Consortium as important centers for harmonization and standardization of rules.[88]

In general, states can act by causing fragmentation of the internet in a number of ways, which have been explored throughout this study. Their motives are even more diverse and may even be grounded in national security and interest, which often repre-

84 WEBER, Rolf H. Legal Interoperability as a Tool for Combatting Fragmentation. Global Commission on Internet Governance, Paper Series: No. 4, Dez 2014, p. 5-6. Available at <https://www.cigionline.org/sites/default/files/gcig_paper_no4.pdf>. Access on January 27, 2017.

85 WEBER, Rolf H. Legal Interoperability as a Tool for Combatting Fragmentation. Op.cit., p. 6.

86 EUROPEAN UNION. (Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). Official Journal of European Communities, L 178, July 17, 2000, p. 1–16. Available at <https://goo.gl/Mvc8cY> . Access on February 11, 2017.

87 COUNCIL OF EUROPE. Convention on Cybercrime. Budapeste, Nov 2001.

88 WEBER, Rolf H. Legal Interoperability as a Tool for Combating Fragmentation.Op.cit., p. 7-8.

sent reasons why states can act without public transparency. Thus, the implementation of blocking mechanisms may go unnoticed by the general population - even in the face of the fundamental right to freedom of expression, based on several international treaties and national constitutions, most notably Article 19 of the Universal Declaration of Human Rights.[89]

In addition, the creation of "frontiers" on the Internet first appeared in a bottom-up,[90] way, since it started from the initiative of users in search of better experience, based on geographical location. However, countries have exerted a top-down,[91] influence on the control of communications with the outside world.[92] Thus, the recent trend has been the increase of territorial limits on the Internet, which matters to the danger of network fragmentation.

6. Final Considerations

The control of the Internet has gained importance proportional to its expansion and has acquired new contexts in the globalized world. In this work, we discuss the main forms of blocking used today, which are practised by governmental authorities, private entities or individuals with different purposes. In order to understand these forms of blocking and the growing cyberactivism against them, the analysis of the internet neutrality concept, as done in this work, is fundamental. In addition, we try to understand the use of geolocation technologies, which grows abruptly, either because of the improvement of customization to user's experience, making the content more adapted to its access location, or due to attempts to control the content present on the internet .

Parallel to the development of the internet, legal systems are constantly striving to regulate the use of new technologies. The adoption of reasonable and proportionate mechanisms that respect human rights and the essential characteristics of the network, particularly with regard to the risks of fragmentation, is imperative for the regular functioning and expansion of the Internet in the world. After all, the Law seeks to protect against exceptional cases, but it must do so without generalizing the solutions beyond the incidence that justifies it. That is, legal frameworks cannot trivialise abusive practices.

In addition to the cyberactivism against the fragmentation of the internet and the development of the legal systems of each state, there are groups that wish to shape the Internet at will. These groups, usually linked to multinational providers of access and content, seek, through the fragmentation of the Internet, to maximize their profits and influence with each user. Usually, this profit maximization is associated with poor services. Therefore, it is necessary that all sectors that integrate the Internet understand minimally about its operation, so that they can defend their own interests and fight for their rights.

89 "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." UN. Universal Declaration of Human Rights. Available at <https://goo.gl/USrdQT>. Access on February 19, 2017.

90 In general, bottom-up means the processes or mechanisms that part of the lower levels to reach the higher ones, for example, as in an initiative of a certain population that presents a proposal to the rulers.

91 Shortly, top-down holds the opposite direction of bottom-up, that is, practices that depart from the highest and most sophisticated levels, such as governments and international organizations.

92 GOLDSMITH, Jack e WU, Tim. Who Controls the Internet?: Illusions of a Borderless World. Oxford: Oxford University Press, 2006, p. 49-50.

7. References

a. Livros, artigos e teses

BELLI, Luca; DE FILIPPI, Primavera De. The Net Neutrality Compendium: Human Rights, Free Competition and the Future of the Internet. 1ª ed. Suíça: Springer, 2016.

BYGRAVE, Lee A. e MICHAELSEN, Terje. Governors of internet. In: BYGRAVE, L. A.; BING, J. (eds.). Internet Governance: Infrastructure and Institutions. Oxford: Oxford University Press, 2009.

GOLDSMITH, Jack e WU, Tim. Who Controls the Internet?: Illusions of a Borderless World. Oxford: Oxford University Press, 2006.

LESSIG, Lawrence. Code v2.0. Nova Iorque: Basic Books, 2006.

SVANTESSON, Dan Jerker B. Private International Law and the Internet. 3ª ed. Holanda: Kluwer Law International, 2016.

ALVES, Sergio, Jr., The Internet Balkanization Discourse Backfires, SSRN Electronic Journal. Available at <https://ssrn.com/abstract=2498753> Access on February 17, 2017.

FARIS, Robert, VILLENEUVE, Nart, Measuring Global Internet Filtering. In: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds., Access Denied: The Practice and Policy of Global Internet Filtering, Cambridge: MIT Press, 2008

HILL, Jonah Force. A Balkanized Internet?: The Uncertain Future of Global Internet Standards. Georgetown Journal of International Affairs. 2012

LEE, Jyh-An e LIU, Ching-Yi, Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China. Minnesota Journal of Law, Science, and Technology, Vol. 13, No. 1, 2012.

LEE, Jyh-An, LIU, Ching-Yi, LI, Weiping, Searching for Internet Freedom in China: A Case Study on Google's China Experience. Cardozo Arts & Entertainment Law Journal, Vol. 31, No. 2, 2013. Available at <https://ssrn.com/abstract=2243205> Access on February 7th, 2017.

LEONARDI, Marcel. Controle de conteúdos na Internet: filtros, censura, bloqueio e tutela. In: mbito Jurídico, Rio Grande, XII, n. 67, ago 2009. Available at <https://goo.gl/rndS2V>. Access on January 30, 2017.

MURDOCH, Steven, ANDERSON, Ross, Tools and Technology for Internet Filtering.. In: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds., Access Denied: The Practice and Policy of Global Internet Filtering, Cambridge: MIT Press, 2008.

WEBER, Rolf H. Legal Interoperability as a Tool for Combatting Fragmentation. Global Commission on Internet Governance, Paper Series: No. 4, Dez 2014. Available at <https://goo.gl/QAT6RT>. Access on January 27, 2017.

b. Legal codes and other reference materials

ARGENTINA. Law 27.078. Argentina Digital Law. Available at <https://goo.gl/qGzigf>. Access on February 10th.

BEREC. BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules. Available at <https://goo.gl/jwjwhI>. Access on February 10th, 2017.

_____. Comunicado de imprensa: O BEREC publica Linhas de Orientação sobre neutralidade de rede (net neutrality), de 30 de agosto de 2016. Disponível em: <https://goo.gl/gPL2bb>. Acesso em 10 de fevereiro de 2017.

_____. What is zero-rating? Available at <https://goo.gl/4MAvqd>. Access on February 13, 2017.

_____. Decree No 8,771 of May 11, 2016. Regulates Law No. 12,965, of April 23, 2014, to deal with the admitted cases of discrimination of Internet data packets and traffic degradation, indicate the safekeeping and protection of data by connection providers and applications, point to measures of transparency in the request of cadastral data by the public administration and establish the parameter for the inspection and verification of infractions. Available at <https://goo.gl/5Dikve>. Access on February 13, 2017.

_____. Law No 12,965, of April 23, 2014. Which establishes the principles, guarantees, rights and duties for the use of the Internet in Brazil. Available at: <https://goo.gl/C7K-I9J>. Access on February 6th, 2017.

CHILE. Law No 18,168. General Telecommunications Law. Available at: <https://goo.gl/ZaDRFY>. Access on February 6th. 2017.

COUNCIL OF EUROPE. Convention on Cybercrime. Budapeste, Nov 2001.

COUNCIL OF EUROPE. Geo-blocking: Council agrees to remove barriers to e-commerce. Available at <https://goo.gl/FGv0jV>. Access on February 12, 2017.

Facebook está preparando lançamento do Free Basics no Brasil. Canaltech, April 14, 2016. Available at: <https://goo.gl/vRT9ff>. Access on February 10th, 2017.

Federal Communications Commission. Open Internet. Available at:<https://goo.gl/sRHoNZ>. Access on February 6th, 2017.

Free Basics by Facebook. Available at: <https://goo.gl/bcPVMz>. Access on February 10th, 2017.

GARATTONI, B. Índia proíbe novo serviço do Facebook; veja por que. Super Interessante, February 22, 2016. Available at: <https://goo.gl/gJwDKY>. Access on February 10th, 2017.

GOMES, Helton Simões. Internet chega pela 1ª vez a mais de 50% das casas no Brasil, mostra IBGE. G1, São Paulo, April 6, 2016. Available at: <https://goo.gl/SZZpcJ>. Access on February 16, 2017.

Mark Zuckerberg anuncia drones para Free Basics. Soluciones Telcel, 26 de fevereiro de 2016. Available at: <https://goo.gl/QOJ08j>. Access on February 10th, 2017.

UNITED NATIONS. Universal Declaration of Human Rights. Available at: <https://goo.gl/YpZwYW>. Access on February 19, 2017.

Parlamento Europeu aprova neutralidade da rede e extingue roaming entre países do bloco. O Globo, Amsterdã, April 3, 2014. Available at: <https://goo.gl/KZOSQD>. Access on February 10, 2017.

Programa de internet gratuito é proibido no Egito. O Globo, Cairo, December 30, 2015. Available at: <https://goo.gl/xSBTrB>. Access on February 10, 2017.

SANTOS, Vinicius W.O. Como a Índia baniu o zero rating. Observatório da Internet no Brasil, February 11, 2016. Available at: <https://goo.gl/Go1wBE>. Access on February 13, 2017.

European Union. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). Official Journal of European Communities, L 178, July 17, 2000, p. 1–16. Available at: <https://goo.gl/9gDKV7>. Access on February 11, 2017.

_____. Office of the Body of European Regulators for Electronic Communications .Available at: <https://goo.gl/LXsMbS>. Access on February 10th, 2017.

_____. Proposal for a Regulation of the European Parliament and of the Council on addressing geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC. Available at: <https://goo.gl/u9oh0a>. Access on February 12, 2017

_____. Regulations, Directives and other acts. Available at: <https://goo.gl/stoDN4>. Access on February 10th, 2017.

_____. EUROPEAN UNION. Regulamento (UE) 2015/2120 do Parlamento Europeu e do Conselho de 25 de novembro de 2015 que estabelece medidas respeitantes ao acesso à Internet aberta e que altera a Diretiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas e o Regulamento (UE) nº 531/2012 relativo à itinerância nas redes de comunicações móveis públicas da União. P. 1. Jornal Oficial da União Europeia L 310/1, November 26,

2015. Available at: <https://goo.gl/xloHrF>. Access on February 10, 2017..