DOI: 10.12818/P.0304-2340.2017vBlp195

NETWORK NEUTRALITY: PAST, PRESENT AND FUTURE OF INTERNET

NEUTRALIDADE DA REDE: PASSADO, PRESENTE E FUTURO DA INTERNET

Leonardo Parentoni[*]

ABSTRACT

The scope of this article is to analyse net neutrality. It starts by contextualizing internet's birth, its purposes, the main principles used on its design and how was the original architecture of that network, specially its modular structure and layers. Next, it describes some recent changes on the internet's structure, highlighting the monitoring and control of data packets, by accessing its headers or using a technology known as DPI (deep packet inspection), which allows the monitoring of the content of each packet, in order to discriminate between them. This part explains how this subject affects the life of billions of people, worldwide. Finally, the paper focuses on net neutrality, as the main legal response to the previously described problems, explaining how it derivate from the original design principles of internet, in order to support a conclusion that reconciles, at one side, free competition and investment strategies, and, at the other side, privacy, freedom of speech, innovation and internet users decision-making autonomy.

KEYWORDS: Internet. Network. Design. Network Neutrality. Innovation.

RESUMO

Este texto aborda a neutralidade de rede (net neutrality). Principia-se contextualizando como a internet surgiu, quais eram os seus propósitos, quais foram os princípios utilizados em seu design e como era a arquitetura originária da rede, principalmente a modularidade e a estruturação em camadas. Na sequência, são descritas algumas das principais mudanças pelas quais a internet vem passando, nos últimos anos, com destaque para o monitoramento e controle dos pacotes de dados, seja através dos headers, seja por meio das tecnologias DPI (deep packet inspection), que permitem monitorar o próprio conteúdo dos pacotes de dados, viabilizando o tratamento discriminatório entre eles. Explica-se como essas mudanças afetam a vida de bilhões de pessoas, em âmbito mundial.

Por fim, aborda-se a neutralidade de rede, como principal resposta regulatória a essas mudanças, a fim de preservar o potencial inovador e o compartilhamento de conteúdo típicos da internet. Frisa-se que a neutralidade de rede decorre dos próprios princípios utilizados no design original da internet, devendo ser interpretada em sintonia com eles, a fim de compatibilizar, de um lado, a livre concorrência, as estratégias empresariais e suas vantagens competitivas; e, de outro, a privacidade, liberdade de expressão, inovação e a autonomia decisória dos usuários.

PALAVRAS-CHAVE: *Internet. Design de rede. Neutralidade da Rede. Inovação.*

* PhD in Corporate Law at USP/Brazil. Master in Law at UFMG/Brazil. LLM in Civil Procedures at UnB/Brazil
Member of Attorney General's Office in Brazil (AGU). Professor of Law at UFMG and at IBMEC/MG. Full profile in English available at the Brazilian Official Database: http://lattes.cnpq.br/3612200644224606. E-mail: parentoni@gmail.com

1 INTRODUCTION AND DELIMITATION OF THE SUBJECT.

This text does not only bring legal considerations. Nor it brings only considerations related to the Information Technology, as the author has no specific training in this last area. Rather, it seeks to merge both, understanding that their joint analysis is essential to understand the actual functioning of the Internet and, with that, propose legal solutions that are plausible and feasible, not only from a theoretical point of view, but especially in the factual aspect. After all, the best theory is the one that works in practice.

Based on this premise, it is intended to address the origins of the Internet and its unique features, responsible for turning it into the success it is today. Afterwards, it is shown how the Internet has been changing in recent years, and the consequences of this change in people and entrepreneurs' lives and in the proper functioning of markets.

Then it is discussed the aspect that, in the author's view, is the main regulatory response to the new problems: the network neutrality. Network neutrality is conceptualized with foreign legal literature and the treatment of the subject brought by the Brazilian Civil Rights Framework for the Internet is also analysed. Finally, the author presents his understanding of how should the network neutrality be applied.

2 BRIEF HISTORIC OF THE INTERNET.

The remote origin of the Internet pushes back to the 50s of the last century, long before its worldwide expansion. Like any other technology, it was the result of a socioeconomic context, which directly influenced the form and the goals for which it was developed. Understanding this point is essential to critically analyse the Internet of today[1].

Indeed, the world was living the so called "cold war", a clear conflict between the United States and the Soviet Union. During this period, the fastest means of communication was by telephone. The telephone network, however, was very vulnerable to military strikes. Aware of this weakness, the US Department of Defense wanted to develop a safer alternative. That's when a systems programmer at Rand Corporation, named Paul Baran, suggested, *still in the 50s*, a computer network model similar to the internet. The Department of Defense, then, consulted with AT&T, the company that monopolized the telephone communication of the country, to figure out if she would be interested in developing this model. AT&T immediately rejected the idea, affirming that it was not feasible[2].

Then, in October 1957, the Soviet Union took a worldwide reported step towards technological progress, launching the Sputnik satellite. In reaction to this, the then US President, Dwight Eisenhower, developed, in September 1959, within the Department

1 CASTELLS, Manuel. **La Galaxia Internet**. Translation: Raúl Quintana. Barcelona: Plaza & Janés Editores, 2001. p. 23. "(...) la producción de una determinada tecnología en um momento histórico condiciona su contenido y los usos que se hacen de ella en su desarrollo futuro. Internet no escapa a esta regla. La historia de Internet sirve para comprender su evolución posterior."

2 TANENBAUM, Andrew S.; WETHERALL, David J. **Computer Networks**. 5th Ed. Boston: Pearson, 2011. p. 55. "Around 1960, the DoD [Department of Defense] awarded a contract to the RAND Corporation to find a solution. One of its employees, Paul Baran, came up with the highly distributed and fault-tolerant design (…) Baran proposed using digital packet-switching technology. Baran wrote several reports for the DoD describing his ideas in detail. Officials at the Pentagon liked the concept and asked AT&T, then the U.S. national telephone monopoly, to build a prototype. AT&T dismissed Baran's ideas out of hand. The biggest and richest corporation in the world was not about to allow some young whippersnapper tell it how to build a telephone system. They said Baran's network could not be built and the idea was killed."

of Defense, an agency for advanced research projects (Advanced Research Projects Agency - ARPANET), dedicated specifically to improve the communication nets. The objective was to overcome the Soviet Union.

Among other purposes, the ARPANET would develop a safer communication network that could remain available even when one of its components got damaged (eg. in case of destruction of a military base, the information stored in it would remain accessible)[3].

However, at that time, the ARPANET had a modest infrastructure[4]. Therefore, *it appealed to the academic world* to develop their objectives[5]. Professors and students then rescued the ideas of Paul Baran, demonstrating the feasibility of establishing a computer network based on the standard that had been suggested by him years before[6].

In the 70s there were already several Local Area Networks (LANs) at the United States of America, but they were not interconnected. For example, at universities. Or even the private networks BBS type (Bulletim Board Systems)[7]. The challenge

3 Op. cit. p. 45-46. "Given the DoD's [Department of Defense] worry that some of its precious hosts, routers, and internet-work gateways might get blown to pieces at a moment's notice by an attack from the Soviet Union, another major goal was that the network be able to survive loss of subnet hardware, without existing conversations being broken off. In other words, the DoD wanted connections to remain intact as long as the source and destination machines were functioning, even if some of the machines or transmission lines in between were suddenly put out of operation. Furthermore, since applications with divergent requirements were envisioned, ranging from transferring files to real-time speech transmission, a flexible architecture was needed."

4 Op. cit. p. 56. "ARPA had no scientists or laboratories; in fact, it had nothing more than an office and a small (by Pentagon standards) budget. It did its work by issuing grants and contracts to universities and companies whose ideas looked promising to it."

5 The first academic institutions to take part at the Net were the *University of California*, Los Angeles, and the *Stanford Research Institute*, in October 1969. Right after, the U*tah University* and the *California University*, in Santa Barbara, also took part at it.

6 Highlighting the importance of academics for the development of internet: HAFNER, Katie; LYON, Matthew. **Where Wizards Stay Up Late**: The origins of the internet. New York: Simon & Schuster, 1996.

7 A famous BBS in the 80s was BITNET, which stands for "because it's there newtwork", evidencing that this kind of net was already a reality.

was to develop a *universal communication standard,* capable of interconnecting all networks and giving birth to a "network of networks". For this purpose, the ARPANET began to promote research in the field, which resulted, in 1978, in the creation of the TCP/IP protocols, which are still the standard of the Internet[8]. Based on them, the various local networks got integrated and started to allow an exchange of information and academic experiences never seen before. A few years later, in the late 80's, the number of institutions, devices and people connected was already so great that the ARPANET was replaced by a more robust network called NSFNET (National Science Foundation Network), reaching across the country. The Internet was taking off from its military origins[9].

At this point, it would not be feasible to keep the Internet under the sole responsibility of the US Government. Then, it was created a private company controlled by the State (ANS - Advanced Networks and Services), to manage the progressive transfer of the network to commercial exploitation ("privatization" of the Internet). This *was consolidated in the 90s*, when many private companies were already acting as access providers[10]. It was also at this time that the network expanded worldwide. That is, effective internationalization of the Internet and its commercial exploitation have started about 40 years after the first researches on the subject.

This brief historic intended to demonstrate that the Internet *was not created as a market-led initiative*. On the contrary, AT&T, a company that monopolized the US telephone communications, showed complete disinterest in the technology in the 50s. In fact, the worldwide web was the result of a partnership between the US Government and educational institutions of the country. Its birth is

8 CASTELLS, Manuel. **La Galaxia Internet**. Translation: Raúl Quintana. Barcelona: Plaza & Janés Editores, 2001. p. 25. "Para conseguir que las redes de ordenadores pudieran comunicar entre ellas, eran necesarios unos protocolos de comunicación estandarizados. (...) En 1978, Cerf, junto con Pastel y Cohen, que trabajaban en la University of Southem California, dividieron el TCP en dos partes, añadiendo el protocolo interredes (IP) y creando así el protocolo TCP/IP estándar sobre el que aún opera Internet."

9 ARPANET was definitively shut-down in February1990.

10 TANENBAUM, Andrew S.; WETHERALL, David J. **Computer Networks**. 5th Ed. Boston: Pearson, 2011. p. 60.

both military and academic[11]. As summed up by Manuel CASTELLS (2001, p. 31)[12]: "*the Internet was born in the unusual crossroad between big science, military research and the libertarian culture.*"

As it will be analysed below, this historical feature was of major importance for the success of the worldwide web.

3 WHAT IS INTERNET MADE OF? NETWORK DESIGN AND ITS LAYERS.

In order to build something, one needs to not only define how the building will be, but also materialize this idea through a project. The architecture/design is the preliminary step to the implementation of the work. With regard to computer networks, this step is called the network architecture or network design[13]. It is the network architecture that defines how the entire infrastructure[14]

11 PARENTONI, Leonardo. **Documento Eletrônico***:* Aplicação e Interpretação pelo Poder Judiciário. Curitiba: Juruá, 2007. p. 27-29.

12 CASTELLS, Manuel. **La Galaxia Internet**. Translation: Raúl Quintana. Barcelona: Plaza & Janés Editores, 2001. p. 31. "Internet nació en la insólita encrucijada entre la gran ciencia, la investigación militar y la cultura libertaria."

13 VAN SCHEWICK, Barbara**. Internet Architecture and Innovation**. Massachusetts: Mit Press, 2010. p. 20-21. "[architecture] denotes the fundamental structures of a complex system as defined during the early stages of product development. Similar to the way the architecture of a house is different from the house itself, the architecture of a system is not the final, working system; rather, it is a description of the system's basic building blocks. (…) In short, the architecture describes the components of the system, what they do, and how they interact."
See also: LESSIG, Lawrence. **Code**: Version 2.0. New York: Basic Books, 2006. p. 24; e TANENBAUM, Andrew S.; WETHERALL, David J. **Computer Networks.** 5th Ed. Boston: Pearson, 2011. p. 31. "A set of layers and protocols is called a network architecture. The specification of an architecture must contain enough information to allow an implementer to write the program or build the hardware for each layer so that it will correctly obey the appropriate protocol."
Also: WHITT, Richard S. A deference to protocol: Fashioning a three-dimensional public policy framework for the internet age**. Cardozo Arts & Entertainment Law Journal**. New York: Benjamin N. Cardozo School of Law. v. 31, n. 03, p. 689-768, Jul. 2013. p. 704. "'Architecture' is a high-level descriptor of a complex system's organization of basic building blocks, its fundamental structures. How the Internet runs is completely dependent on the implementing software code, its fundamental nature created and shaped by engineers."

14 About the concept of infrastructure see: OLIVEIRA, Raquel Diniz; PARENTONI, Leonardo. Uma Advertência sobre Interoperabilidade e o Artigo 154, Parágrafo Único,

of a computer network will be, affecting its functioning and even the cost and the possibilities for future modification.

There are several possibilities for network architecture. It will depend on the direction followed by its creators. This direction, in turn, is given by the design principles[15]. In the development of the Internet, there were applied four fundamental principles: 1) Packet switching; 2) Modularity; 3) Network layers; and 4) End-to-end.

Understanding the original design of the Internet is essential to perceive how it has been changing and what are the consequences of these changes.

Indeed, the basic feature of the internet is to divide the data into smaller fractions, called packets, transmitting them separately. Each packet receives information about who is the sender and what is the address (*addressing*). Hitherto, something similar to traditional mail, on paper. The big difference is that the various packets can travel simultaneously by several routes, even changing the route along the way, to privilege the one that is faster and more effective (*switching*). Getting to the destination, the packets are reassembled to form the original data and then delivered. This principle enables the data transmission even if one or a few network components are disconnected, congested or by any reason unavailable[16]. This was the solution suggested by Paul Baran in the 50s, and subsequently endorsed by the US Government, through ARPANET. The following figure compares traditional data communication, via direct cable connection, with packet switching:

---

do CPC. **Revista Magister de Direito Civil e Processual Civil**. Porto Alegre: Magister, Ano IV, n.º 19, p. 51-73, jul./ago. 2007.

15 VAN SCHEWICK, Barbara. **Internet Architecture and Innovation**. Massachusetts: Mit Press, 2010. p. 23. "A design principle describes known connections between architectural choices and the characteristics of the resulting architecture. (…) a design principle describes how to design an architecture for a system with specific quality characteristics, and, like different versions of a dish, the resulting architectures will differ depending on the design principles that were used to create them."

16 ROBERTS, Lawrence Gilman. The evolution of packet switching. **Proceedings of the IEEE.** New York: IEEE Foundation. v. 11, p. 1307-1313, Nov. 1978. p. 1307. "[A packet switched network] divides the input flow of information into small segments, or packets, of data which move through the network in a manner similar to the handling of mail but at immensely higher speeds."

Figure 1 Alternative routes of communication through internet

It is noticed that the difference is the possibility that the data from "A" to "B" is delivered, even if the direct connection between them is compromised, as there is the option of using the route through "C". On the internet, for each route there are hundreds or even thousands of alternatives. The following figure illustrates how the data is broken during transmission and then reassembled at the destination:

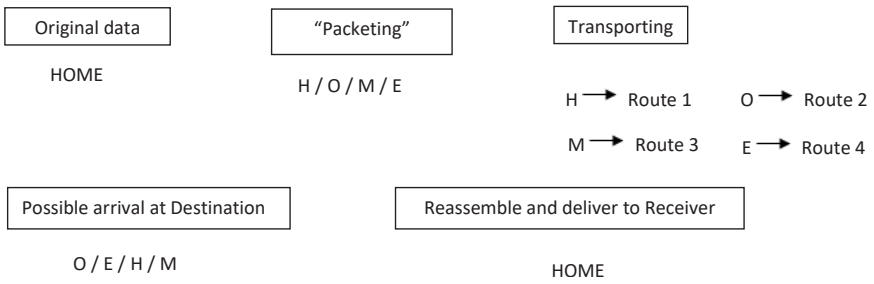

Figure 2 Data communication through packet switching

The second principle applied at the original internet design was *modularity*. Based on it, the network consists of many parts, independent of each other, called modules[17]. The intention is to reduce to a minimum the dependence of the network as a whole upon each component. For this reason, every module has two types of information, the visible and the "invisible"[18]. *Visible information*

17 VAN SCHEWICK, Barbara. **Internet Architecture and Innovation**. Massachusetts: Mit Press, 2010. p. 38. "Modularity is a design principle that intentionally makes components highly independent ('loosely coupled'). Components of modular designs are called modules. When designing a modular architecture, system architects decompose the system in a way that minimizes dependencies among components."

18 TANENBAUM, Andrew S.; WETHERALL, David J. **Computer Networks**. 5th Ed. Boston: Pearson, 2011. p. 29. "The fundamental idea is that a particular piece of

is one that any component of the network needs to know in order to connect with a particular module. It should remain unchanged and available to any interested party during whole life of the network, in order to not disrupt communication between modules. For example, the VGA port format, used for monitors connection to PCs, is a visible data. Knowing this information, any manufacturer is able to produce a monitor that supports this port.

On the other hand, the necessary information for the internal operation of each module is called *"invisible" information*. It is usually known only by the module manufacturer, consolidating its competitive advantage over competitors. For example, the resolution and mode of operation of the monitor. As long as the visible information remains the same, modules with different internal configurations are compatible. That is, the same PC could connect to many monitors. Another example is the USB port. Holding the visible information (format of the port and what is needed to connect to it), any manufacturer can develop a compatible product, such as mice, printers, cameras, mobile phones, tablets, etc. The fact that each product has a different internal setting does not affect the connection. *The great advantage of modularity is to allow internal improvements in each component of the network with no need to change its entire infrastructure*[19].

In turn, communication between the various modules is established through its internal specifications (*protocols*[20]) and through connection to the layers that are immediately higher and lower (*services*[21]). Thus, network layers are arranged vertically (*stack*

software (or hardware) provides a service to its users but keeps the details of its internal state and algorithms hidden from them."

19 It steps aside from the "*all or nothing*" logic, allowing ponctual modifications, as well as reducing the adaption cost of each modification.

20 TANENBAUM, Andrew S.; WETHERALL, David J. **Computer Networks**. 5th Ed. Boston: Pearson, 2011. p. 29. "Basically, a protocol is an agreement between the communicating parties on how communication is to proceed."

21 Op. cit. p. 40. "Services and protocols are distinct concepts. (…) A *service* is a set of primitives (operations) that a layer provides to the layer above it. The service defines

of layers[22]) with relative independence from one another.

Yochai Benkler believes that any communication system should present at least 3 layers[23]. Specifically in what regards the internet, there is no consensus about how many layers there are and which would they be, and there is more than one classification[24]. *In this paper, the description comprising 6 layers was chosen:* 1) Physical; 2) Of Connection (data link); 3) Of Network; 4) Of Data Transport; 5) Of Applications; and 6) Of Content.

The initial layer from the bottom up, is the physical. She encompasses the devices that transmit data in its raw form (raw data), such as network cables, satellites and mobile phone towers[25]. Next, comes the connection layer, responsible for establishing the connection between the devices that transmit the raw data and the

---

what operations the layer is prepared to perform on behalf of its users, but it says nothing at all about how these operations are implemented. A service relates to an interface between two layers, with the lower layer being the service provider and the upper layer being the service user.
A *protocol*, in contrast, is a set of rules governing the format and meaning of the packets, or messages that are exchanged by the peer entities within a layer."

22 Op. cit. p. 29. "To reduce their design complexity, most networks are organized as a stack of layers or levels, each one built upon the one below it. The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network. The purpose of each layer is to offer certain services to the higher layers while shielding those layers from the details of how the offered services are actually implemented."

23 BENKLER, Yochai. From consumers to users: Shifting the deeper structures of regulation toward sustainable commons and user access. **Federal Communications Law Journal**. Washington: George Washington University Law School. v. 52, n. 03, p. 561-579. 2000.

24 Depending on the classification, certain layers are assembled or disassembled. There are, for example, those who consider that the physical layer would not be a part of the network itself, as it does not correspond to one of its modules, merely transmitting the data in raw form (*raw data*).

25 YOO, Christopher S. Protocol Layering and Internet Policy. **The University of Pennsylvania Law Review**. Philadelphia: The University of Pennsylvania. v. 161, n. 06, p. 1707-1771. 2013. p. 1747. "Any path that can convey a message sequence can constitute a link in this layer, whether physical or not. The means of encoding information varies widely depending on whether the carrier wave is composed of visible light passing through a fiber optics network, an electromagnetic wave passing through a copper wire, or an electromagnetic wave passing through the ether."

network itself[26]. The third layer is the one that assigns identification to the data, through the *internet protocol* (IP)[27]. In effect, any device connected to the internet must have an identification number. It is through this number that the IP protocol individualizes the device, ensuring that it properly sends and receives data. In a simplified way, the IP address works for the Internet such as the home address of the person works for the post office. Each device has a unique IP, but the same person may have multiple devices connected to the network simultaneously, each one with a different IP. For example, mobile phone, PC, tablet etc. What matters is to individualize the devices, not their holder[28].

After identifying the data with the source and the destination IPs (end hosts), the fourth layer is responsible for effectively transmitting them[29]. This is done through another protocol called TCP (*Transfer Control Protocol*). It is this protocol that fraction the original data into smaller packets and, in the sequence, transmits them.

The IP and the TCP work together, consolidating the heart of the Internet[30]: one individualizes the data by inserting the source

26 Op. cit. p. 1746. "Data-link layer protocols share with network-layer protocols the responsibility for guiding traffic through the network; as a result, data-link layer protocols necessarily run in switches as well as hosts."

27 Op. cit. p. 1745. "(…) this layer provides the uniform basis that each network connected to the Internet uses to transmit data communications across an ever-changing landscape of technologically heterogeneous systems."

28 TANENBAUM, Andrew S.; WETHERALL, David J. **Computer Networks**. 5th Ed. Boston: Pearson, 2011. p. 43. "The network layer controls the operation of the subnet. A key design issue is determining how packets are routed from source to destination." The possibility of a dynamic IP does not interfere in this reasoning because in every connection the device will have a specific IP. There will only be no guarantee that the following connection uses the same number.

29 Op. cit. p. 44. "The basic function of the transport layer is to accept data from above it, split it up into smaller units if need be, pass these to the network layer, and ensure that the pieces all arrive correctly at the other end."

30 SOLUM, Lawrence B.; CHUNG, Minn. The Layers Principle: Internet Architecture and the Law**. Notre Dame Law Review**. Notre Dame: University of Notre Dame Law School. v. 79, n. 03, p. 815-948, Jan. 2004. p. 839. "Without TCP/IP there can be no Internet."

and the destination addresses; the other splits the data, transmits and reassembles them at the destination. For that reason, it is common to hear "TCP/IP protocol" (in the singular), when in reality they are two different[31] and complementary things (a protocol suite).

The fifth layer network is the applications one[32]. On this layer all software and typical features of the Internet are run (in programming language), such as the browsers used to access sites, the social networks and the download of files. The end result of these applications is then transmitted to the user, by the sixth and final layer. Most users generally think that the internet is composed only by this last layer, as it represents all they effectively see on the screen of their devices. The lower layers are commonly known and exploited only by the system's programmers and the services providers.

This modular architecture, organized in layers, defines the way the data communication via the Internet is processed. Indeed, there is no direct transfer from a layer, in the source device, to the equivalent layer in the target device. In fact, the communication first flows "top-down", from the device used to generate the data, through TCP/IP, which will individualize, route and fraction them into packets, until they reach the physical layer. From there, they will be transmitted in its raw form until they reach the place in which the receiver is located. After that, they start to flow "from the bottom up", ranging from the physical layer to the connection one, through TCP/IP, which will be responsible to check if the destination is correct and, if so, reassemble the packets, reconstituting the original data, to then send them to the application that will process them (in programming language), until the final result is displayed on the

31 In the origins of the internet it has been proposed to merge both protocols into a single one, the *Internetwork Transmission Control Protocol* – ITCP. However, this idea was soon discarded: VAN SCHEWICK, Barbara. **Internet Architecture and Innovation**. Massachusetts: Mit Press, 2010. p. 96 a 98.

32 YOO, Christopher S. Protocol Layering and Internet Policy. **The University of Pennsylvania Law Review**. Philadelphia: The University of Pennsylvania. v. 161, n. 06, p. 1707-1771. 2013. p. 1742. "This layer encompasses a wide variety of protocols, each designed to support particular classes of applications."

receiver device[33]. The following figure facilitates the visualization of this route:

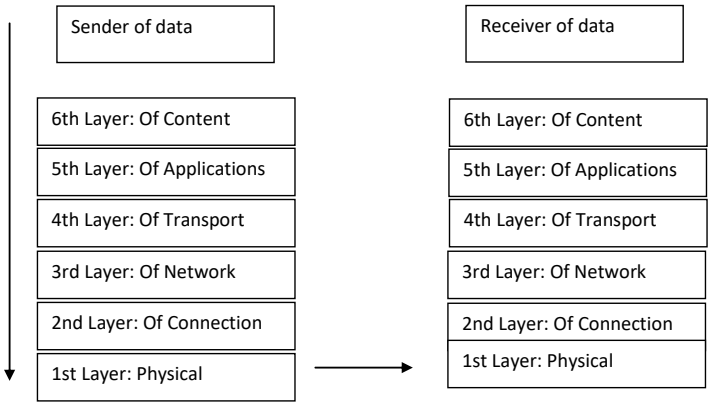

Figure 3. Network layers.

The characteristic feature of this network architecture is that the core layers, such as TCP/IP, are not able to identify the content of the transmitted data. For them, it is not a concern whether the data represent a legal text, a journalistic article or any other manifestation of thought. The type of application to which they relate is also indifferent. For example, if they relate to a web page, to the transmission of a movie or to a post on a social network. The same and universal standard is followed for the transporting of *any* data, directed to *any* kind of application[34]. The applications, located at the penultimate upper layer, are the sole responsible for identifying the content of the data and for what purpose they should be applied to. This is the fourth and final design principle used in the construction of the Internet: Running Applications in the Upper Layer (*end-to-end*). Opposite option is that one in which the functioning of the

33 SOLUM, Lawrence B.; CHUNG, Minn. The Layers Principle: Internet Architecture and the Law. **Notre Dame Law Review**. Notre Dame: University of Notre Dame Law School. v. 79, n. 03, p. 815-948, Jan. 2004. p. 816-817.

34 VAN SCHEWICK, Barbara. **Internet Architecture and Innovation**. Massachusetts: Mit Press, 2010. p. 72. "[This] results in a network that is not able to distinguish between the different applications running over it, or to control or to positively or negatively affect their execution."

applications is controlled by the central layers of the network (core centered). This option was *not* used on internet's original design.

The simplicity in the operation of the central layers of the internet, coupled with the absence of filters, allows any new application to be immediately and worldwide disseminated, without requiring any further adjustment in the basic network infrastructure[35]. For this reason, the Internet has become a major conductor, open to the transmission, sharing and collective construction of various types of content, stimulating innovation and dialogue[36]. *The success of the internet, therefore, is closely related to the original design of the network*.

On the other hand, as the internal specification of each module remains visible only to its manufacturer (hence hidden from all other services that connect to this module), the integration between them is not the best possible. There are, thus, *loss of performance* in the modular architecture model, if compared with the full integration of the network components.

These advantages and disadvantages of the original internet architecture will be discussed with further detail later. For now, it is enough to highlight that there is no perfect alternative, capable of providing only qualities. The network design necessarily involves a trade-off between losses and gains.

35 Op. cit. p. 140. "In an end-to-end network (such as the original Internet) in which network operators and application designers follow the broad version of the end-to-end arguments, designing, implementing, testing, and deploying a new application do not require changing the network's core (…)."
Obviously, this rule is not absolute. Certain applications, to present an acceptable performance, may eventually require structural changes in the network. This is the case of streaming of audio and video, as well as the peer-to-peer applications.

36 RANCHORDÁS, Sofia. Does Sharing Mean Caring? Innovation in the Sharing Economy. **Minnesota Journal of Law, Science & Technology.** Minneapolis: The University of Minnesota. v. 16, n. 01, p. 01-63, winter. 2015. p. 14-15. "Innovation is a broad concept that can be defined differently depending on the context and field in question. (…) innovation is defined as 'the ability to take new ideas and translate them into commercial [or effective social] outcomes by using new processes, products, or services (…)'. Innovation is more than an idea or a novelty; it must be the first successful concretization of an idea in the marketplace or in society."

4 HOW IS INTERNET CHANGING.

In the previous topics, it has been demonstrated that the internet is a *human construction*, guided by certain *principles and objectives*[37]. Like any other human construction, it can be altered. After all, there are other possible settings, each one guided by different social, political and economic purposes[38]. It happens that, depending on the type of change, and on the intensity with which it is implemented, this can give rise to a new internet, entirely different from the one the world has used to know. This topic intends to, briefly, point out some of these changes. In the next topic it will be done a critical analysis about them, in the legal perspective.

It is known that the phone lines were built focusing, primarily, at the transmission of sounds. Just as TV cables were designed only to the service of paid TV. None of these technologies were designed to the internet typical data flow, especially because the internet was developed later. Consequently, the transmission speed for the internet applications was originally very low. Subsequent changes in these instruments, however, have made possible the transmission of data at speeds until then unforeseeable, which rendered these new technologies the name "broadband"[39]. Thus, copper cables were gradually replaced by optical fibre, whilst traditional phone lines evolved to ADSL (asymmetric digital subscriber line)[40]. The same

37 LESSIG, Lawrence. **Code**: Version 2.0. New York: Basic Books, 2006. p. 06. "We can build, or architect, or code cyberspace to protect values that we believe are fundamental. Or we can build, or architect, or code cyberspace to allow those values to disappear. There is no middle ground. There is no choice that does not include some kind of building. Code is never found; it is only ever made, and only ever made by us."

38 LEMOS, Ronaldo. Uma Breve História da Criação do Marco Civil. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III**: Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. I. p. 79.

39 TANENBAUM, Andrew S.; WETHERALL, David J. **Computer Networks.** 5th Ed. Boston: Pearson, 2011. p. 95-111.

40 In Brazil, for instance, the companies "Oi" and "GVT" provide access via ADSL, whilst "NET" and "SKY" use the optical fibre cable system. In less urbanized regions of the country, where telephone networks and cabling are still precarious, alternative access technologies, through radio or satellite, are often used.

has occurred in relation to the internet access through the electricity transmission networks, satellites, radio waves, microwaves or WiFi (wireless fidelity).

Each of these technologies, in their own way, and for different backgrounds, allowed the improvement of the internet-trough communications. The common element that have to be highlighted is that *all of them could be implemented only in the physical and in the connection layers, without the need of entirely altering the network operation*. Hence, Internet-connected devices remained fully interoperable. This was only possible thanks to the original layered design and to the modularity.

Throughout the evolution of the internet, several other modifications were made solely in the *application layer*, also *preserving the core of the network*. There were created, for instance, protocols for the direct file transfer between devices (*file transfer protocol* - FTP) and the communication via e-mail (*simple mail transfer protocol* - SMTP).

One of the most impactful change in how the internet is used was the development of the DNS (*domain name system*)[41]. It has been already said that every device connected to the network has an IP address. To access the device, it would then be necessary to type this address, consisting in numerical sequences, such as "200.251.4.1". However, such sequences are difficult to memorize and they may change over time. This made surfing at the internet extremely complex. It was difficult for people to memorize a sequence like this for each site they commonly accessed, and check if the numbers had not changed.

In order to solve this problem, there was an application capable of associating each IP address to a specific name, so that typing the name replaced typing the numeric address. This application is called DNS. She is responsible for the fluid and

41 TANENBAUM, Andrew S.; WETHERALL, David J. **Computer Networks**. 5th Ed. Boston: Pearson, 2011. p. 611-612.
Also: MACIEL, Rafael Fernandes. A Requisição Judicial de Registro de Conexão e Aplicações no Marco Civil. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III:** Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. II. p. 478.

intuitive way navigating on the network currently is, by simply typing "www.google.com" or "www.facebook.com" to access sites, whatever their IP numbers are. The DNS was not part of the original architecture of the network and was introduced later on, shortly before its commercial exploitation.

Another important recent change, which also has been unnoticed by most Internet users, is the transition from IPv4 to IPv6. Indeed, IPv refers to the IP protocol *version* that, as described, serves to individualize devices on the network by assigning them an IP address. When the internet was created, the version number 4 of this protocol (IPv4) was adopted[42] and, in accordance to it, addresses were formed by four numerical sequences, each one ranging from 0 to 255. For example, "200.251.0.1". This version allowed approximately 4.29 billion devices to be simultaneously connected. It may seem a lot, but it is not. Knowing that the tendency is that more and more individuals and companies have access to the internet, and that each one can consume alone, tens or even hundreds of IP addresses, then it follows that the total number of addresses was doomed to someday end[43].

When this comes to happen, the internet would be "crowded", preventing the addition of new users and/or devices[44]. To overcome this problem, another version of the IP protocol was developed, called IPv6[45]. Through IPv6 it is possible to offer, simultaneously, a few trillion times the maximum number of addresses supported by IPv4. An impressive amount, which will be hardly overwhelmed,

42 Technical description at: UNITED STATES OF AMERICA. The Internet Engineering Task Force – IETF. Available at <https://tools.ietf.org/html/rfc791>. Access on 21st March 2016.
The three previous versions were used in the network early days, when it was still restricted to the US.

43 This could take decades longer to happen if certain IP addresses had not been assigned, collectively, to some US institutions, far above their needs.

44 Phenomenon dubbed *IPcalypse* in a jocular allusion to the Apocalypse of the internet. Available at: <http://www.ipcalypse.net/>. Access on 21st March 2016.

45 Technical description at: UNITED STATES OF AMERICA. The Internet Engineering Task Force – IETF. Available at <https://tools.ietf.org/html/rfc2460>. Access on 21 March 2016.

even if the number of network-connected devices increases[46].

IPv6 is based on the hexadecimal system, combining letters and numbers. This new protocol is being implemented gradually, coexisting with IPv4. For example, the email address "www.facebook.com" corresponded, in March 2016, to the IPv4 "200.175.89.139" and to the IPv6 "2A03: 2880: 2130: CF24: face: b00c: 0: 25de66.220.158.68"[47].

Hitherto it has been pointed out some changes that are happening at peripheral layers of the Internet (physical, connection and applications layers). None of them, however, reached the heart of the network, to the point of changing the principles of the original design, such as the operation of TCP/IP protocols. It happens that this kind of change - much more serious and controversial - is also already happening. It consists on the introduction of technologies for monitoring the package *content* itself (*deep packet inspection* - DPI)[48].

The DPI is a software capable of examining both the packet routing's information (headers), which indicate its source and destination, and the actual content of each data packet. This occurs when the data are passing through a given point in the network, where the software is programmed to act[49]. From this point on, it is possible to *discriminate packets*, defining whether they should proceed or be discarded, as well as imposing different speeds for each transmission. The access to headers is necessary and legal, because

46 It is estimated that IPv6 addresses allows to form more addresses than the total number of atoms in the universe: MELANCIA, André. O crescimento da Internet. **Revista Programar**. Available at: <http://www.revista-programar.info/artigos/ipv6-para-programadores/>. Access on 9th April. 2016.

47 The use of dynamic IPs was not taken into account, to simplify the example.

48 GEIST, Michael. The Emergence of Net Neutrality Regulation in Canada: How Canada Developed a Consensus Policy on One of the Internet's Most Contentious Issues. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III**: Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. II. p. 646. "The DPI [deep packet inspection] capabilities allow ISPs to identify the type of content that runs on their networks and render it possible for them to manage the traffic based on the content."

49 Such programs are normally operated by the internet service providers.

it is essential to the flow of data on internet. What the law forbids is the discrimination between packets, based on this information.

This was *inconceivable* in the origins of the internet. As seen, the worldwide web was designed under the principle of modularity, to ensure interoperability with any new program or hardware, without requiring changes to the network infrastructure (the original modules) or to its layers. As long as the external information of each module remained the same, an infinite range of new modules could be connected.

Not only that, but *the TCP/IP protocols worked neutrally,* transmitting any data packets, regardless of their origin, destination or of which given species they were. Only at the top layer of the network that data would be identified, by each particular application, in order to generate the final result (a movie, music, text etc.). During the transmission, it shall be reinforced, it was absolutely irrelevant to which sort of data it was.

It turns out that this has changed. Currently, much of the physical infrastructure of the internet belongs to the private sector[50]. Thus, it is no surprise that private interests are behind the major recent changes in the network operation. One of the most controversial is precisely the introduction of the DPI. From this technology on, the internet service providers have gained a previously inconceivable power. They are able to manipulate the way users sense the network, providing greater speed to some data packets over others. Or even interrupting the transmission of certain packets. Taking up the example of the Post Office, it is as if providers could read all the posted correspondence, choosing whether and when to deliver each one. The recipient would tend to

50 VERGUEIRO, Luiz Fabricio Thaumaturgo. Marco Civil da Internet e Guerra Cibernética: Análise Comparativa à Luz do Manual de Talin Sobre os Princípios do Direito Internacional Aplicáveis à Guerra Cibernética. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III**: Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. II. p. 634-635. "(...) The core of the Interent is formed by a series of infrastructure elements: ithe nterconnection points (IXP), the backbones or national stems, regional networks and local networks, in general, are in owned by private entities, in a way that its openness and its technology contains elements with potential for internal control."

think that some services were more efficient than others, as some of the correspondence relating to them (for example, payment slips), always arrive first, whilst others tend to delay. Now picture the range of business, political and ideological interests that could abide such discrimination.

Practices of this sort, by the Post Office, would sound absurd and unacceptable. However, on the internet, they are already taking place, and with great frequency. Worst of all, many users do not even know it[51]. This structural change in internet *has misrepresented its main feature*, which was precisely the neutrality of the TCP/IP protocols in what regards the transmission of content. In the original design of the network, the packet identification was restricted to the upper layer applications, where each data packet was assigned for a specific purpose (end-to-end principle). The core of the network, composed by the TCP/IP protocols, worked neutrally, without worrying about the content of the packets or who would be their sender and recipient.

The next topic will seek to demonstrate how this structural change in the core network layers leads to very serious and worldwide consequences, both micro and macroeconomic.

5 HOW DOES IT AFFECT YOUR LIFE?

But after all, how this issue affects *your* life?

The subject of this text not only interest large corporations, even though it also interests them. Neither it affects solely the systems programmers or the engaged internet users (known as "activists"). It affects the lives of *all* people who use, have used, or someday might make usage of the internet[52]. In essence, billions of

51 GEIST, Michael. The Emergence of Net Neutrality Regulation in Canada: How Canada Developed a Consensus Policy on One of the Internet's Most Contentious Issues. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III**: Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. II. p. 650. "Yet, the public generally remained somewhat apathetic towards the issue, with the net neutrality debate crowded by 'telecom lobbies'."

52 Only in Brazil, about 86 million people frequently use the internet: CAPUTO, Victor.

people around the world. This subject affects, indirectly, even those who do not have access to the World Wide Web[53]. The problem has micro and macroeconomic outcomes, both in country's internal and international levels, being able to meddle with the organization and functioning of markets[54].

In fact, the network architecture has direct influence in the costs of possible alterations of it in the future[55]. In the case of Internet, its original design used to provide *low costs for innovations*, because new products or services, as a rule, would require only changes in the top layer, on the applications, remaining intact all others[56]. Of course this rule is not absolute, since certain types

---

Mais da metade dos brasileiros são usuários da internet. **Caderno Tecnologia, Revista Exame**. Available at <http://exame.abril.com.br/tecnologia/noticias/mais-da-metade-dos-brasileiros-sao-usuarios-da-internet>. Acess 07 April 2016.

53 Imagine a resident of an underdeveloped country, who has never accessed the Internet, but that could be hired as an employee of a startup, whose business model is based on the internet. The income from this job would have been a means of improving the living conditions of this citizen and his family. However, he may never have this chance, once the structural changes of the internet can make the aforementioned startup not exist.

54 COMPARATO, Fábio Konder. Capitalismo e Poder Econômico. **Revista da Faculdade de Direito da UFMG**. Belo Horizonte, special number: em memória do Professor Washington Peluso Albino de Souza, p. 167-195, 2013. p. 169. "What is properly called market, and that have always been the center of the attention of classical political economy, is the open space of distribution of goods and the provision of services, where imperates the law of division and specialization of tasks."

55 VAN SCHEWICK, Barbara. **Internet Architecture and Innovation**. Massachusetts: Mit Press, 2010. p. 116. "(…) the number and the kinds of components that need to be changed to realize a particular innovation may differ among architectures. As a result, realizing that innovation may be more expensive in one architecture than in another."

56 Op. cit. p. 151. "The Internet was designed to interconnect subnets regardless of their physical network technology. (…) To connect a new type of subnet to the Internet, all one needs is a router that can connect this type of subnet to a physical network that uses an existing network technology.
(…)
These design choices make it possible to innovate on application-layer protocols (as long as no other application-layer protocols depend on them) and on link-layer protocols (as long as the IP service interface stays the same) without any system-adaptation costs, both when new protocols are added and when existing protocols are innovated upon."

of innovation in the application layer also require changes in the lower layers of the network, to ensure good quality of the services. For example, the transmission of video in real time (*streaming*), has required certain improvements in the physical and connection layers, so that the increase in the data stream would not overload the network. Even in the TCP/IP layers it would require, eventually, changes in the protocols, in order to adapt them to new applications. IPv6, mentioned above, is a good example. What should be clear is that, in all these cases, the original network design - and the principles that guided its creation - has been *preserved*.

By contrast, in networks that have integrated design, the cost of any alteration tends to be higher, since it is not enough to change just one or a few modules, being necessary to adapt the entire infrastructure[57]. And the higher the cost, the more difficult it becomes to small entrepreneurs to launch new products or services. Consequently, integrated networks present two disadvantages: 1) they make innovation more expensive; and 2) they tend to concentrated the innovation in a small group of people, precisely the ones that have sufficient resources to bear the costs of major changes in the network infrastructure.

Thus, the architecture of a computer network certainly influences *who* is able to innovate. But it doesn't stop there. It also affects some other aspects. Considering that the costs of innovation are prohibitive for small entrepreneurs, it tends to concentrate the innovation only on large companies such as Google, Facebook, Apple and Microsoft. So these companies' interests are the ones that will guide *what* should be created and *when*[58].

57 Op. cit. p. 121. "Owing to the different levels of coupling between components, the costs of realizing a specific innovation probably will be greater in an integrated architecture than in a modular architecture."

58 RAMOS, Pedro Henrique Soares. O Marco Civil e a Importância da Neutralidade de Rede: Evidências Empíricas no Brasil. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III:** Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. II. p. 149. "In an extreme model, the strengthening of the core of the architecture can lead to a similar communication model, of what happened in traditional television - even if users have the choice to change the channel, the communication flow has primarily one direction, and the decisions on content availability and the use of applications will be restricted

Considering only fully integrated network architecture, creations that today bring immense comfort and satisfaction to users, such as WhatsApp and Skype, would probably not exist. What these applications have in common is the fact that they have emerged as an alternative to traditional communication, just as telephone, which is why they have faced strong resistance from mobile telephony operators. As it can be assumed, those operators would not have developed something that, at the time, would conflict with their own business model.

Thus, the creation of these applications was only possible thanks to the original design of the Internet. In this model, *the creative power is shifted* from the center (large companies) to the end (the final users). As long as any user can make use of the pre-built network infrastructure, without the need for adjustments, it becomes considerably easier and cheaper to develop new products or services and, immediately, to make them available to the market, possibly even worldwide. Mark Zuckerberg, founder of Facebook, for example, payed the first servers that hosted the famous social media for only $85.00 per month[59].

Even when external financing is needed, the modular architecture seems to be more advantageous. It allows the capture of funds to be done in an alternative form, other than the financial market, and also the reduction of costs, such as in crowdfunding[60]. This *gives greater freedom and flexibility to developers*, since they don't need to submit to external interferences in their ideas and business plans, what would inevitably occur if they were to depend

---

to the interests of those who manage the core network."

59 VAN SCHEWICK, Barbara. **Internet Architecture and Innovation**. Massachusetts: Mit Press, 2010. p. 206.

60 MARTINS, Norberto Montani; DA SILVA, Pedro Miguel Bento Pereira. Funcionalidade dos sistemas financeiros e o financiamento a pequenas e médias empresas: o caso do *crowdfunding*. **Revista Economia Ensaios.** Uberlândia: EdUFU. v. 29, especial edition (Associação Keynesiana Brasileira), p. 25-56, Dez. 2014. p. 26. "(...) It can be said that crowdfunding is an alternative form of financing, that connects, directly through the internet and social networks, those that can offer, lend or invest resources with those in need of funding for projects or specific business. Moreover, the collective funding is characterized by the fact that the projects and businesses mentioned are financed by small contributions of a large number of individuals, anonymously."

on investments coming from investment funds or large companies.

The original design of the Internet, that provides the capability of innovation described above, even against the will of the large companies in the sector, is suffering several changes. And the current changes are much deeper than those experienced in the past. Depending on the type and the way they are consolidated, they may compromise: 1) innovation; 2) freedom of expression; 3) privacy; and 4) the proper functioning of markets.

In this context, if the internet had not been designed based on packet switching, modularity, layering and running applications in the upper layer, it certainly would not have become what it is today. Features and applications that the world is now used to, simply would not exist. And worst of all, people would not notice or miss them, because they wouldn't have even tried these features...

An example illustrates this perfectly. Today, the peer-to-peer (P2P)[61] technology is consolidated and provides easy file sharing, for many different purposes[62]. However, when it was developed, it suffered harsh attacks and it only survived thanks to the original design of the Internet.

The first online platform that allowed users to share free music, worldwide, was Napster[63]. This application was strongly based on P2P technology. With its success and rapid growth, Napster was sued by the US recording industry, since the songs were being transferred without paying copyrights[64]. This lawsuit resulted in

61 KRISHNAN Ramayya; SMITH, Michael D.; TELANG, Rahul. The Economics of Peer-To-Peer Networks. **Journal of Information Technology Theory and Application.** Las Vegas: The University of Nevada. v. 05, n. 03, p. 01-24. 2003. p. 01. "P2P networks allow a distributed community of users to share resources in the form of information, digital content, storage space, or processing capacity. The novel aspect of these networks is that, in contrast to client-server networks where all network content is located in a central location, P2P resources are located in and provided by computers at the edge of the network (...)."

62 Some of these purposes, of course, are illegal. However, this does not mean that P2P technology is harmful. After all, every technology tends to be neutral. The usage that we make of them is what makes it good or bad.

63 Further details can be found at: WU, Tim. When code isn't Law. **Virginia Law Review**. Charlottesville: Virginia Law Review Association. v. 89, n. 04, p. 679-751, Jun. 2003.

64 A&M Records, Inc. v. Napster, Inc. Case n° 00-16401. 239 F.3d 1004. United States Court of Appeals for the Ninth Circuit. Decided in October, 2, 2000.

the extinction of the company. Despite of that, the P2P technology was not affected. The case preserved the original configuration of the internet, since its effects were restricted to the upper layer of the network, specifically affecting only the Napster application.

Because of that fact, the P2P technology remained available and, through it, were developed several other products and services with huge success and without the Napster illegality vices. Skype is one of them. Other services highly based on technology still bring legal challenges such as Uber[65] and Airbnb[66]. But it is a fact that it would not have been possible the emergence of any of them if, because of the Napster case, the infrastructure of the Internet, in its lower layers, had been affected in order to stop the P2P.

However, changes like that are currently taking place with enough intensity and speed. The belief that the unique features of internet will always remain the same has already been surpassed[67]. It is undeniable that, in recent years, it has undergone changes with the clear purpose of enabling *greater control and monitoring*[68]. One

---

To learn more about this case: PARENTONI, Leonardo. **Documento Eletrônico***:* Aplicação e Interpretação pelo Poder Judiciário. Curitiba: Juruá, 2007. p. 178-184.

65 Open content. Wikipedia: the free encyclopedia. "Uber". Available at: <https://pt.wikipedia.org/wiki/Uber_%28empresa%29>. Access on 3rd April 2016. "Uber is an American multinational corporation of urban private transport, based on disruptive technology networked through an e- hailing app that offers a similar service to the traditional taxi, popularly known as 'paid ride' services.
(...) E- hailing is the act of ordering a taxi through an electronic device, usually a mobile phone or smartphone. It replaces traditional methods to call taxis, such as phone or simply wait or go looking for a taxi on the street."

66 Open content. Wikipedia: the free encyclopedia. "Airbnb". Avaiable at: <https://pt.wikipedia.org/wiki/Airbnb>. Access on 3rd April 2016. "Airbnb allows individuals to rent the entire place or part of his own home, as a form of extra accommodation. The site provides a search platform and reserves to occur between the person who provides the accommodation and the tourist who search for rental. It covers more than 500,000 adds, in over 35,000 cities and 192 countries.

67 About this topic: BARLOW, John Perry. **A Declaration of the Independence of Cyberspace**. Available at: <https://projects.eff.org/~barlow/Declaration-Final.html>. Access on 28th December 2015.

68 As an example: LESSIG, Lawrence. **The Law of the Horse***:* What cyberlaw might teach. *Harvard Law Review*. New York: Aspen Law and Business, n.º 113, p. 501-549, Dec. 1999; LESSIG, Lawrence. *Code*: Version 2.0. New York: Basic Books, 2006; ZITTRAIN, Jonathan. **The Future of the Internet**: And how to stop it. London:

of the most aggressive changes is the interference in the TCP/IP protocols, replacing the original feature of neutrality for monitoring data packets, not only in its origin and destination, but also in relation to the actual content of each package. *A side effect of this is the possibility of differentiating the data stream, according to certain interests*.

In the case of China, for example, those interests are political in nature and seek to institutionalize censorship. This way, the Chinese government interferes in the network layers in order to block access to any sites that, supposedly, contain "inappropriate content", which means any political content contrary to the government's own interests[69]. This is possible since all the big connection providers of international networks (backbones[70]) in China, are all subject to strict governmental supervision and control. These providers ensure that IP addresses from China remain blocked from accessing certain foreign sites, especially newspapers and news websites[71]. In a jocular analogy with the famous Walls of China, this practice became known worldwide as The Great Firewall of China[72].

Yale University Press, 2008; RODOTÀ, Stefano. **A Vida Na Sociedade da Vigilância**. Translation: Maria Celina Bodin de Moraes. Rio de Janeiro: Renovar, 2008.

69 LEMOS, Ronaldo. Uma Breve História da Criação do Marco Civil. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III**: Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. I. p. 79. "The way the network is legally treated in different countries has very different orientations. And not always democratic values guide that relationship. In this context, the Internet is not a network disconnected from the existing political systems. Instead, more and more politics and law have influence in the evolution of the Internet and how it is governed and administered."

70 TANENBAUM, Andrew S.; WETHERALL, David J. **Computer Networks**. 5th Ed. Boston: Pearson, 2011. p. 64. "At the top of the food chain are a small handful of companies, like AT&T and Sprint, that operate large international backbone networks with thousands of routers connected by high-bandwidth fiber optic links. These ISPs do not pay for transit. They are usually called tier 1 ISPs and are said to form the backbone of the Internet, since everyone else must connect to them to be able to reach the entire Internet."

71 To know if a site is blocked in China, it is possible to test it, typing: Great Firewall of China. Available at: <http://www.greatfirewallofchina.org/>. Access on 4th April 2016.

72 SOLUM, Lawrence B.; CHUNG, Minn. The Layers Principle: Internet Architecture and the Law. **Notre Dame Law Review**. Notre Dame: University of Notre Dame Law

Not only the states have interfered in the functioning of the internet. The market also does that. Major international players such as Google, Microsoft, Facebook, Apple and other of the same gender continuously monitor the network usage. The intention is to identify consumption habits and, with that information, to draw a profile of Internet users that is able to facilitate the sale of products and services completely focused on them[73]. In this context, the data acquired considerable economic value[74], being primarily responsible for paying services that are apparently free, such as e-mail accounts or social networks. In all these cases, the payment is made indirectly. Instead of paying cash, the traditional way, it allows service provider to have access to user privacy and to make profit from it[75]. It is the economic interest guiding the discrimination of the data stream.

School. v. 79, n. 03, p. 815-948, Jan. 2004. p. 896-910.

73 About this topic: BAKER, Stephen. **Numerati.** Translation: Ivo Korytowski. São Paulo: Saraiva, 2009

74 DE FRANCESCHI, Alberto; LEHMANN, Michael. Data as Tradeable Commodity and New Measures for their Protection. **The Italian Law Journal**. Napoli: Edizioni Scientifiche Italiane. v. 01, n. 01, p. 51-72, Mar. 2015. p. 51. "Information, particularly important, significant and relevant information, (…) is today's 'digital gold'."
The "Letter of Fundamental Rights of the European Union has been amended to emphasize the importance of personal data in this new context: EUROPEAN UNION. European Parliament and Council of the European Union. Letter of Fundamental Rights of the European Union. Strasbourg 12 December 2007. Available at < http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:12012P >. Access on 4th April 2016.

75 LEONARDI, Marcel. Marco Civil da Internet e Proteção de Dados Pessoais. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III:** Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. I. p. 528. "(…) As is known, the advertisement is directed, which was made possible by the treatment of user data - personal or otherwise - that sustains the system of services and the free information online. Other business models subscriptions, micropayments, closed sites - did not have the same success with the majority of users, that were used to 'all free' online. Between paying a small fee for access, per day or per month, or giving personal data, almost all users prefer to pay with their data.
Paying with data is a valid choice and must be respected, is a model that allows all users to participate in the online system, not just those who have the resources to pay for content and services."
Having in mind that reality, today it is said that we lived in the Big Data era: MAYER - SCHÖNBERGER, Viktor; CUKIER, Kenneth . **Big Data**. New York: HMH, 2013.

Another form of discrimination based on economic interest is traffic shaping. It consists in increasing the speed and quality of the service and, at the same time, reducing the competitors, to damage the latter. This causes the end user the false impression that a service is better than other. Imagine, for example, an Internet connection provider (responsible for the speed and connection quality) which is also - directly or through a company of the same economic group - the provider of streaming video service. Thanks to the changes that the Internet has had, in recent years, this provider can reduce the access speed of its members for competing services, affecting their quality in order to induce them to use the service of the access provider itself. In Brazil, NET (connection provider) could increase the speed of the Now service (its video streaming) and, at the same time, to reduce the speed and quality of Netflix (main competitor). In this context, subscribers of NET would have the false impression that the Now is much better than Netflix. In other countries, such practices have resulted in bitter judicial disputes[76].

Another kind of traffic shaping occurs when the Internet access provider deliberately reduces the speed of certain applications, not to benefit with service that it also provides, but simply because they want to difficult the use of these applications. This is very common in relation to P2P. The difference from the Napster case is that now it is not only about simply combating some applications based on this technology, using the argument that it stimulates fraud. The proper functioning of the internet has been changed to harm the whole P2P, whatever are the applications that are using it or their purposes.

76 In the US, for example, the country's largest connection provider (Comcast) artificially reduced the speed of the main competing service (Netflix), in order to induce customers to opt for the service provider itself (NBC).
The case took to a lawsuit that ended with an agreement in which Netflix had to pay extra values to Comcast, so the company would not reduce the speed of access of its members to the service provided by Netflix. Following, the other competitors were forced to seek similar agreements with Comcast.
USA. Comcast Corp. versus F.C.C. United States Court of Appeals for the District of Columbia. 600 F.3d 642, j. 06.04.2010.

To justify this, the argument of the access providers is that P2P is typically used to transmit large data packets, which could overload the network, decreasing the speed available for other applications. As metaphor, the internet could be seen as a great avenue. The more cars traveling at the same time, the slower the general flow of traffic would tend to be. The cars in this metaphor would be the data packets and P2P would represent the slow trucks that catch the flow of other vehicles. The following topics will show that this argument is false[77].

For now, it is important to note that the traffic shaping clearly subverts the original features of the internet. It tends to accentuate the formation of monopolies and the concentration of economic power, reducing the innovations and the sharing of content, especially those coming from small developers. It also means indirect censorship, once the user finds himself prevented from using certain applications, with quality and speed that could be expected of them, because of unilateral choice of the connection providers. This has a direct impact on *who* will be able to innovate, *what* will be created, *when* there will be innovation and based on what values/goals. It affects, therefore, the lives of billions of people and the functioning of the Internet, worldwide. How is the law reacting to all of this? This is the subject of the next topic.

6 THE MAIN REGULATORY RESPONSE: NETWORK NEUTRALITY.

The change in the internet infrastructure is attracting attention from various fields of science, including the legal area, considering the amount of consequences it can cause. The main legal response to this problem is known as the principle of *net neutrality*[78].

77 To avoid the overload of the network, there are alternatives that do not lead necessarily to the P2P restriction. The usage of symmetrical bandwidth, replacing the current asymmetric band model, would be one of them: VAN SCHEWICK, Barbara. **Internet Architecture and Innovation**. Massachusetts: MIT Press, 2010. p. 69-70.

78 WU, Tim. Network Neutrality, Broadband Discrimination. **Journal of Telecommunications and High Technology Law**. Boulder: The University of Colorado, v. 02, n. 01, p. 141-176, Fall. 2003. p. 165. "[network neutrality exists to] to forbid

According to this principle, the Internet service providers - especially access providers (ISPs)[79] - can not, within certain limits, discriminate the data packets that travel through its infrastructure, because of the origin, destination or content of the data. Thereof, this measure seeks to preserve the full access to information and the decision-making autonomy of Internet users, in a way that they are not illegally manipulated to opt for a particular product or service.

The net neutrality is a worldwide controversial subject[80]. In Brazil, the embryo of this principle was already included in the General Telecommunications Law[81]. After long and heated debates, the issue was also included in the Brazilian Civil Rights Framework for the Internet, in April 2014. This law included the net neutrality as

broadband operators, absent a showing of harm, from restricting what users do with their Internet connection, while giving the operator general freedom to manage bandwidth consumption and other matters of local concern. The principle achieves this by adopting the basic principle that broadband operators should have full freedom to 'police what they own' (the local network) while restrictions based on inter-network indicia should be viewed with suspicion."
GEIST, Michael. The Emergence of Net Neutrality Regulation in Canada: How Canada Developed a Consensus Policy on One of the Internet's Most Contentious Issues. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III**: Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. II. p. 641. "While the definition of net neutrality is open to some debate, at its core is the commitment to ensuring that Internet service providers (ISPs) treat all content and applications equally with no privileges, degrading of service or prioritization based on the content's source, ownership or destination. (…) Adopting a neutral approach, in other words, requires strict adherence to one cardinal rule: that ISPs transport data without discrimination, preference, or regard for content."

79 LEONARDI, Marcel. **Responsabilidade Civil dos Provedores de Serviços de Internet**. São Paulo: Juarez de Oliveira, 2005. p. 23. "The ISP is the company that provides, as a service, the access to the Internet for their customers. Typically, these companies have a connection to a backbone or operate their own infrastructure for direct connection."

80 In the Us, the public debate about this topic, between Tim Wu (advocate of the neutrality) and Chitopher Yoo (against it), was extremely relevant for the matter: WU, Tim; YOO, Christopher S. Keeping the Internet Neutral? Tim Wu and Christopher Yoo Debate. **Federal Communications Law Journal**. Bloomington: Indiana University Maurer School of Law. v. 59, n. 03, p. 575-592, June. 2007.

81 BRAZIL. National Congress. Law n. 9.472. Brasília: 16 July 1997. "Article 3. The user of the the communication services have the right to:
(...)
III – not to be discriminated about the conditions of access and usage of the services".

a principle on the use of the Internet in Brazil, dedicating a specific section to this topic:

> Article 3. The discipline of Internet use in Brazil has the following principles:
> (...)
> IV - preserving and safeguarding network neutrality;"
>
> Article 7. Access to internet is essential to the exercise of citizenship and users are assured the following rights:
> (...)
> V - to the maintenance of the hired quality of internet connection;
> VI - to clear and complete information contained in the services contracts, with details on the arrangements for protecting the connection logs and access records to Internet applications, as well as network management practices that can affect its quality;
>
> CHAPTER III
> THE PROVISION OF CONNECTION AND INTERNET APPLICATIONS
> SECTION I
> THE NETWORK NEUTRALITY
>
> Article 9. The agent in charge of transmission, switching or routing is obliged to treat any data package with isonomy, regardless of content, origin and destination, service, terminal or application.
> § 1st – The discrimination or degradation of traffic will be regulated in accordance to the private assignments of the president of the republic provided in item IV of the article 84 of the constitution, to the faithful implementation of this law, being heard the internet steering committee (CGI) and the national agency of telecommunications (ANATEL), and may only arise from:
> I – technical requirements essential for the adequate provision of services and applications; and
> II – emergency services prioritization.
> § 2nd - In the event of discrimination or degradation of traffic referred to in paragraph 1, the aforementioned agent must:
> I – to refrain from causing damage to users, as regarded in article 927 of the civil code;
> II – to act with proportionality, transparency and equal protection;
> III – to inform previously the users in a transparent, clear and sufficiently descriptive manner about its management and traffic mitigation adopted practices, including those related to network security; and
> IV – to provide services on non-discriminatory commercial conditions and refrain from practicing anticompetitive behaviors.
> § 3rd - In the provision of internet connection, onerous or for free, as well as in the transmission, switching or routing, it is forbidden to

> block, monitor, filter or analyze the contents of data packets, respected the provisions of this article[82].

Network neutrality was one of the most controversial points of the Brazilian Civil Rights Framework for the Internet, and it was discussed throughout the whole legislative process[83]. If the interception of electronic communications scandal in several States by the Government of the United States (known as case Edward Snowden)[84] haven't happened, perhaps today the Brazilian Civil Rights Framework for the Internet would not have been approved in Congress. Mainly because the priority, in the following years, was the serious economic and political crisis that took place in the country.

In general, the Brazilian legal literature has proven favourable to the Brazilian Civil Rights Framework for the Internet, although there are, of course, some critics[85] to the way the network neutrality

82 BRAZIL. National Congress. Law n. 12.965. Brasília: 23 April 2014.

83 For a detail history of this topic: LEMOS, Ronaldo. Uma Breve História da Criação do Marco Civil. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III**: Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. I.

84 Open content. Wikipédia: the free encyclopedia. "Edward Snowden". Available at: <https://pt.wikipedia.org/wiki/Edward_Snowden>. Access on 4th April 2016.

85 Some examples of harsh critics: FILHO, Eduardo Tomasevicius. O Marco Civil da Internet e as Liberdades de Mercado. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III**: Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. II. p. 59-60.
"In theory, this neutrality claim may be beneficial to Internet users in Brazil, but it also may have little practical effect because, because if the network is global, with data traffic from one point to another of the world, the neutrality would not have much use if other countries have not required the neutrality of their networks in their territories. It does not seem possible for the data to flow in Brazil with neutrality if the same data is transferred in different conditions in the networks of other countries. (...)
It should be noticed that the Brazilian Civil Rights Framework for the Internet, did not consider the regulations that already existed in the General Telecommunications Law (Law 9472 of July 16, 1997). The art. 3 of that law already guaranteed users of telecommunications, among other rights, 'III - not to be discriminated against on the conditions of access and enjoyment of the service' (...).
Thus, any anti-competitive or discriminatory practices coming from the Internet connection providers, which could adversely affect the market freedom, did not result

was treated. It is understood that this law - despite it being timely and relevant - is not an end in itself. It represents just another step towards the legal regulation of the subject. In order to reach its objectives, the net neutrality, according to the view of this author, must: 1) be contextualized according to the original design of the Internet and its infrastructure; and 2) have clear limits.

It is worth noticing, besides, that almost in the end of the her government, less than 24 hours before being removed because of the impeachment proceedings, the President Dilma Rousseff edited a Decree[86] regulating the Brazilian Civil Rights Framework for the Internet, referring to two controversial issues: 1) net neutrality; and 2) the processing of personal data.

Despite the possible censorship referring to this moment - political and legal - based on which this Decree was published, the rules that it contains, generally, are in accordance with the ideas defended in this essay and can be considered a breakthrough in the topic.

In the next topic, these issues will be best addressed.

of the absence of applicable legislation, but rather of the inefficiency in combating such practices. Besides, the regulation of the General Telecommunications Law is more precise than the the one of the Brazilian Civil Rights Framework for the Internet, in which they used intentionally vague terms and terms with little semantic content, precisely to facilitate its adoption as an ordinary law by the National Congress."

86 BRAZIL. President of the Republic. Decree n. 8.771. Brasília: 11 May 2016.

7 INTERNET DESIGN AND THE LIMITS OF NETWORK NEUTRALITY.

Both in Brazil[87] and in the world[88], the debate over network neutrality is highly polarized. On one side, there are those that *oppose* to it. They argue, essentially, that the absolute neutrality runs counter to the basic notion of market because it eliminates the competitive advantages, discouraging investment in research and innovation. After all, what motivates innovation is exactly the temporary monopoly granted by the intellectual property system, so the creator can refund the costs that he had and still make profit. If he does not receive differential treatment to their products, services or processes, rather than the competitors, there will be no incentive to innovate. Those who share this opinion also argue that the differential treatment to certain data packets is inner to the management of computer networks, in a way that a fully neutral network would have low quality of services and which could lead to the dissatisfaction of the users. Certain controls are necessary, for example, as in the packet filtering in order to avoid spam[89], or when it seeks to prevent that only a few users (heavy users) consume all the connection[90]. These and other arguments are typical of Internet

87 RAMOS, Pedro Henrique Soares. O Marco Civil e a Importância da Neutralidade de Rede: Evidências Empíricas no Brasil. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III**: Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. II. p. 152. "The issue of net neutrality often brings ideological views and discourse that has little to do with scientific research. Business, political activists, lobbyists and lawmakers, although playing valid roles within the political debate, often carry his speeches with shallow arguments and little empirical evidence that, in no way, contribute to go deeper in the debate on the effects of regulation of net neutrality for the society."

88 For both arguments in favor of and against net neutrality, see: LENARD, Thomas M; MAY, Randolph J (Coord.). **Net Neutrality or Net Neutering**: Should Broadband Internet Services Be Regulated? New York: Springer, 2006.

89 PARENTONI, Leonardo. SPAM: presente, passado e futuro. **Revista de Direito das Comunicações**. São Paulo: Revista dos Tribunais, ano 3, n. 5, p. 13-48, jan./jun. 2012. "(...) Spam is the electronic message that has direct or indirect commercial nature, and that is massively sent to multiple receptors, consciously, with uniform content and without any potential interest to the receptor."

90 The excessive use of peer-to-peer applications, for example.

access providers and large companies in the telecommunications industry. Ultimately, these agents intend to ensure full freedom to administer the connection of the users, as they see it is the best.

At the other extreme are the *advocates* of the network neutrality. Generally, some governments, non-governmental organizations, some engaged Internet users and some academics. They argue that net neutrality is consistent with the original design of the Internet, being largely responsible for the World Wide Web to become the success it is today. Furthermore, they argue that this design is vital to maintain the collaborative nature and innovative potential of the internet. Thus, any filtering of the data packets would be, at first, harmful. Even those filtering that are based on security reasons or in the network management should be justified and adopted only in exceptional cases. In addition, the packet filtering could lead to censorship or illegally restriction of the user's choices, as in the case of traffic shaping. Therefore, the ones in favour believe that the scope of the net neutrality should be expanded as much as possible.

This essay is not linked to any of these extremes. In fact, it considers that both bring relevant arguments, which must be taken into consideration in order to understand the limits of network neutrality. It seeks, in this context, an *intermediate route*, which recognizes the need to preserve the competitive advantages of the entrepreneurs (whatever their economic size might be) and, at the same time, to allow independent developers and ordinary people to use the internet as a tool for innovation and for sharing content. In this sense, *what is proposed is a legal regulation that first understands the functioning of the internet and, only then, will set limits to the network neutrality, in accordance with the structural changes experienced in recent years*.

But if the original Internet design was based on certain principles, as discussed in this text, it should also occur with the legal regulation. Two legal principles are worth mentioning: 1) The end-to-end communication; and 2) The preservation of the network layers (layers principle).

From the computer network architecture's point of view, the end-to-end principle is already old and, according to that, the

lower layers of the network must be designed in a way that it can work in the simplest way possible, getting the complexity reserved for upper layer applications[91]. This way, many different applications, with different degrees of complexity, are able to coexist in a way that all of them are benefited from the same standard infrastructure of data, which requires fewer changes in the network, making it more stable. In the case of the Internet, this means that the TCP/IP protocols should have as fewer interventions as possible. Innovation should preferably occur in the upper layer, with the development of new applications.

Bringing this topic to the legal analysis, decades later, this principle states that *the legal regulation of the Internet should focus on the application layer, preserving, as much as possible, the original design of the other network layers*[92]. The Napster case, already mentioned, is a good example. Focusing exclusively on the Napster application, it was possible to combat the unlawful conduct, without changing the structure of the Internet or compromising the P2P technology. Thereof, the applications that emerged later made use of P2P to provide new services. On the other hand, the Chinese model makes usage of the TCP/IP protocols for political censorship, which would be prohibited under this principle.

Some authors divide this principle in two different aspects. According to the broad version[93], the end-to-end principle

91 SALTZER, Jerome Howard; REED, D. P.; CLARK, David Dana. **End-to-End Arguments in System Design. ACM Transactions in Computer Systems.** New York: ACM New York, v. 02, n. 04, p. 277-288, Nov. 1984.

92 LESSIG, Lawrence. **Code:** Version 2.0. New York: Basic Books, 2006. p. 44. "Rather than build into this network a complex set of functionality thought to be needed by every single application, this network philosophy pushes complexity to the edge of the network – to the applications that run on the network, rather than the network's core. The core is kept as simple as possible."

93 VAN SCHEWICK, Barbara. **Internet Architecture and Innovation**. Massachusetts: Mit Press, 2010. p. 96. "The broad version of the end-to-end arguments argues that application-specific functionality usually cannot – and preferably should not – be implemented in the lower layers of the network, the network's core. Instead, a function should be implemented in a network layer only if it can be completely and correctly implemented at that layer and is used by all clients of that layer. Thus, lower layers, or the core of the network, should provide only general services of broad utility across

determines that *the lower network layers must provide increasingly standardized and simplified services*. For example, the physical layer (connecting cables) takes care exclusively of the transport of the data in its raw form. The way to connect to it is a standard. Differently, the upper layer, the application one, performs various activities. In this layer, are performed simple and complex tasks, involving the processing of data in order to generate results as text, images, videos, etc. Consequently, *any changes in the network layer should only be made if they can be fully implemented in this layer, without it meaning that the other layers have to be changed too*. And only when these changes are *essential for all services that use this layer*. For example, there is no justification to change the TCP/IP protocols to improve the quality of a specific application, because it is not essential for the operation of the others. This attitude would lead to the disruption of the pattern in the lower layers, adding them unnecessary complexity. Moreover, this kind of change can compromise the simplicity and stability of the network. In the other hand, the replacement of copper cables for the fiber optic ones is a change that can be implemented entirely in the physical layer, benefitting all the users, without increasing the complexity in this layer. This substitution would, therefore, be in accordance with the principle in analysis.

The narrow version[94] of this principle provides that *all changes that cannot be implemented solely in one network layer*, or that would not beneficiate all the services that make usage of this layer, without any distinction, *must be implemented in the application layer, functioning end-to-end*, exclusively between the sender and receiver. Thereof, if any application is developed and it requires a functionality that still doesn't exist (such as a new type of biometric identification), it is necessary that all the technology

applications, whereas application-specific functionality should be implemented in higher layers at the end hosts."

94 Op. cit. p. 90. "The narrow version of the end-to-end arguments postulates that, since certain functions cannot be completely and correctly implemented in lower layers of the network, they must be implemented end-to-end between the end hosts that are the original source and the ultimate destination of data."

required for its operation is inside the application itself. This way, it is enough that the users only have this application installed on their devices so they can communicate, without the need for any change in the internet infrastructure.

Another important legal principle is the preservation of network layers (layers principle[95]). According to this principle, *only in exceptional cases the regulation of one layer can interfere with the operation of the others*. Returning to the case of China, the solution adopted by the government is contrary to this principle because, to combat a problem in the application layer (access to political content), they reached central layers of the network (TCP/IP). An extreme example would be a country that, intending to exercise the maximum control over the Internet, would keep a single access provider, which would be tightly supervised by the State. In this case, instead of focusing only on the application layer, the control is focusing on the connection layer.

The regulation that goes further of the network layer brings two problems that are apparently antagonistic: over inclusiveness and under inclusiveness. Once more referring to the case of China, it is forbidden access to any sites that contain unofficial political content. Nevertheless, many of these sites also provide other information on various subjects, which there is no need to be blocked (excessive coverage). On the other hand, sites that do not directly are dedicated to political discussion, doing it in an indirect way, would be immune to the block (insufficient coverage). Considering all that,

95 SOLUM, Lawrence B.; CHUNG, Minn. The Layers Principle: Internet Architecture and the Law. **Notre Dame Law Review**. Notre Dame: University of Notre Dame Law School. v. 79, n. 03, p. 815-948, Jan. 2004. p. 817-818. "Our thesis is that the design of legal rules should respect a fundamental principle of Internet architecture, which we shall call *the layers principle*. At this stage, we can roughly formulate the layers principle as a rule of thumb for Internet regulators: respect the integrity of the layers. This fundamental principle has two corollaries. The first corollary is the *principle of layer separation*: Internet regulation should not violate or compromise the separation between layers designed into the basic architecture of the Internet. The second corollary is the *principle of minimizing layer crossing*: minimize the distance between the layer at which the law aims to produce an effect and the layer directly affected by legal regulation. (…) The best regulations attack a problem at a given layer with a regulation at that layer. The worst regulations attack a problem at the content layer by imposing a regulation at the physical layer – or vice versa."

the best legal regulation is the one that is directed exclusively to the layer where the problem is - usually the applications layer - without any effect on the others.

Both end-to-end and layers principles are *the basis* of the network neutrality. It is true that the TCP/IP protocols have undergone profound changes in recent years. Its original neutrality has been replaced by a detailed investigation of the packages. Thereof, it becomes necessary to set *legal limits* to avoid the negative consequences of such monitoring. These limits are given precisely by the network neutrality. Thus, it is necessary to systematize it.

The network neutrality – as any other principle – is *not* an absolute value[96]. It should be relativized considering certain *legal reasons* or *factual characteristics* of each network.

Thereof, some factual characteristics of the internet require special treatment for certain data packets, in a way that the final result of the process is satisfactory[97]. For example, the differential treatment is justified, having in mind the nature of the e-mail, in comparison with the streaming of video in real time. The delay of a few seconds to deliver an e-mail does not compromise the functionality of this application. In fact, it is not even noticed by the receiver. In the other hand, constant delays in displaying a video, even for only a few seconds, harms the functionality of this application. From the factual and technical-operational points of view, therefore, the different treatment of these data packets is justified, reserving higher transmission speed to streaming video, compared to email. The Brazilian Civil Rights Framework for the Internet expressly admits this type of discrimination[98], only

96 Remember that, in Brazil, even life is not an absolute value, because even the death penalty is possible in case of war formally declared (CF/88 art. 5º, XLVII, "a").

97 WU, Tim; YOO, Christopher S. Keeping the Internet Neutral? Tim Wu and Christopher Yoo Debate. **Federal Communications Law Journal**. Bloomington: Indiana University Maurer School of Law. v. 59, n. 03, p. 575-592, June. 2007. p. 577. "Yet I don't think that the fact that an absolute ban on discrimination would be ridiculous undermines the case for discrimination laws. It's like what nutritionists say about fat: there are good and bad types. And what I think is going on in the network neutrality debate – the useful part of it – is getting a better grip on what amounts to good and bad forms of discrimination on information networks."

98 BRAZIL. Nacional Congress. Law n. 12.965. Brasília: 23 April 2014. Article 9º, § 1º, I.

for technical reasons, for the sake of a higher quality of services (network management[99]). The Decree nº 8.771/2016, that regulates the Brazilian Civil Rights Framework for the Internet, explains how these limitations can and should occur[100]. It starts by pointing that these limitations only affect the "connection providers and internet applications." They do not reach, for example, "telecommunications services that are not intended for providing internet connection" or those "intended for specific groups of users with strict control of admission," such as private networks (intranets)[101].

Another cause for lawful factual discrimination in the data flow is the *emergency services*[102]. It is even recommended to prioritize data packets that concern them, such as police or public health information, giving them greater speed of transmission. Which ones specifically are these services is a matter that should be included in regulations to be issued by the National Telecommunications Agency - ANATEL[103].

99 BRAZIL. President of Republic. Decree n. 8.771. Brasília: 11 May 2016. "Article 6. For proper delivery of services and applications on the Internet, the network management is allowed in order to preserve its stability, security and functionality, using only technical measures compatible with international standards, developed for the proper functioning of the Internet, and in compliance with regulatory standards issued by Anatel and considered the guidelines established by CGIbr."

100 BRAZIL. President of Republic. Decree n. 8.771. Brasília: 11 May 2016. "Article 1 - This Decree points the admitted discrimination of data packets on the Internet and the traffic degradation; it indicates procedures for data storage and protection by providers of connection and applications; it points transparency measures on the request of information for registration by the public administration; and it establishes parameters for surveillance and investigation of violations of the Law 12.965 of 23 April 2014."
"Article 4. The discrimination or the degradation of traffic are exceptional measures, to the extent that it can only come from necessary technical requirements for the proper provision of services and applications or prioritization of emergency services, requiring the obedience to all the requirements set out in article 9, § 2, of Law n. 12.965/2014."

101 BRAZIL. President of Republic. Decree n. 8.771. Brasília: 11 May 2016. Article 2.

102 BRAZIL. Nacional Congress. Law n.12.965. Brasília: 23 April 2014. Article 9º, § 1º, II.

103 BRAZIL. President of Republic. Decree n. 8.771. Brasília: 11 May 2016. Article 8.

In more exceptional situations, such as a formally declared war, it would be lawful even to interfere with the physical layer and the connection in order to difficult or suppress the access to the internet from the belligerent State. If, as mentioned, even the death penalty is permissible in this context, even more restrictions on the internet are allowed[104].

Anyway, even where technical and operational reasons justify the differential treatment of data, *it is the network administrator's duty to inform the users which are the criteria used and how the various kinds of data will be handled*[105]. Thus, the users would be able to question any positions that might lack in technical basis or that might be disproportionate.

These and other exceptions lead to the conclusion that despite internationally acclaimed, the term "network neutrality" may not be the most appropriate. After all, the Internet nowadays is not neutral. Some distinctions are absolutely necessary and legally permitted. What this principle seeks, in fact, is to prevent and stop *unfair* discrimination. Thereof, the network neutrality prohibits the discriminatory treatment of the same type of data packets, based on

104 VERGUEIRO, Luiz Fabricio Thaumaturgo. Marco Civil da Internet e Guerra Cibernética: Análise Comparativa à Luz do Manual de Talin Sobre os Princípios do Direito Internacional Aplicáveis à Guerra Cibernética. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III**: Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. II. p. 633-634. "Sovereignty means that the State can control the entire infrastructure from cyber activities that develop the onshore portion of its territory, in its internal waters, territorial sea (including seabed and subsoil), archipelagos and the underlying airspace. As a consequence of state sovereignty, the cyber infrastructure should be submited to the legislative and regulatory control of the state, but also the State should protect this infrastructure, if it is private or public property. (...) In the cyber context, the principle of sovereignty allows a state to restrict or protect, in whole or in part, the access to the Internet, considering the other rules of International Law and Human Rights. (...) Similarly, the sovereignty exercised by a State on its territorial sea grants the full control over the laying of submarine cables, which is a crucial factor of control, to the extent that the portion with more massive Internet data currently is supported by submarine cables."

105 BRAZIL. Nacional Congress. Law n. 12.965. Brasília: 23 April 2014. Article 9º, § 2º, III.
BRAZIL. President of Republic. Decree n. 8.771. Brasília: 11 May 2016. Article 5 and article 7.

their content, origin or destination[106]. For example, the distinction between two films, simply because one is from Netflix and other from Net Now. The distinctions can be made in many ways, not only by changing the speed of access to any of these applications, but also, e.g. securing that access to one of them is "free" (in the sense that it will not be deducted from the user's data allowance), while access to others will be normally charged.

Thus, it is fully acceptable that the service providers offer various service packages with different characteristics in each of them. For example, services with lower speed and lower franchise data, cheaper, and services with higher speed and higher deductibles data (or even no deductible), with a higher cost. This is inherent in the market economy. Stratification of a particular service in different levels, with their own characteristics and different costs, is common in many areas, even in the health business, where many different plans could be offered. Moreover, this differentiation is benefic, since each person or group have specific needs and capabilities in terms of payment, and it is not reasonable nor efficient to impose just one model for all.

What is not admitted is that the network administrator, outside the legally permissible exceptions, would handle the connection of its users, having influence, even indirectly, in the way that the service package is used. The choice of how to use the internet access is personal, being done by the users. The ISPs cannot provide the connection in order to direct users to specific applications. This rule, which could already be perfectly understood, in a systematic interpretation of the Brazilian Civil Rights Framework for the Internet, now is properly regulated[107]. Once the connection speed

106 FORGIONI, Paula Andrea; MIURA, Yuriko Rocha. O Princípio da Neutralidade de Rede e o Marco Civil da Internet no Brasil. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III**: Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. II. p. 113-114. "The discussions on the neutrality and the equal treatment of data must take into account that, in the current web architecture, there is already a differentiation of the information that goes trough its structure: equality is applied to identical or similar data, and not to the different applications which, because of its characteristic, require different treatment."

107 BRAZIL. President of Republic. Decree n. 8.771. Brasília: 11 May 2016. "Article 3.

and other technical aspects remain the same, it is the user himself who will decide whether to use Netflix or Net Now, WhatsApp or any other similar application.

In addition, the *network neutrality focuses on the lower layers*, especially the TCP/IP protocols, preserving its full compatibility with any applications that already exist or will exist. *In the application layer, the rule is the free competition*. Each developer can and should create innovative technologies, increasingly complex and specific, exploring them economic and exclusively within the limits of law. In other words, innovation flourishes in the application layer, from end to end, while the network neutrality focuses on the lower layers, ensuring that they are not manipulated to seek unlawful goals.

This way, it is understood that free competition, the business strategies and the competitive advantages can be ensured, on one side, and privacy, freedom of speech, innovation and the decision-making autonomy of users, on the other.

At this point, it is necessary to question the article 2, *caput*, of Decree nº 8.771/2016[108], since it also extends the neutrality to the providers of "Internet applications", i.e., the upper layer. This article suffers from two vices. The first is its *illegality*, since it goes

---

The requirement of an equal treatment brought by article 9 of the Law n. 12.965/2014, must ensure the preservation of the public and unrestricted nature of the internet and the foundations, principles and objectives of Internet use in the country as provided by the Law n. 12.965/2014."
"Article 9. Unilateral conducts or agreements between the responsible for transmitting, switching or routing and application provider are forbidden if:
I - commit the public and unrestricted nature of the internet and the foundations, principles and objectives of Internet use in the country;
II - prioritize data packets due to commercial arrangements; or
III - prioritize applications offered by themselves, that is also responsible for transmitting, switching or routing or by companies that are member of the same economic group. "
"Art. 10. The commercial offers and internet access charging models should preserve a single internet, with open nature, plural and diverse, seen as a way to promote human, economic, social and cultural development, contributing to form an inclusive and non-discriminatory society."

108 BRAZIL. President of Republic. Decree n. 8.771. Brasília: 11 May 2016. "Article 2. The provisions of this Decree are intended to the companies responsible to transmit, switch or route and to the connection and Internet application providers, as defined in the item I of the caput of article 5 of the Law n. 12.965/2014."

further from the Brazilian Civil Rights Framework for the Internet, increasing restriction that was not expressly provided by the law. After all, the article 9 of the Brazilian Civil Rights Framework for the Internet is clear in providing that net neutrality applies to the "responsible for transmitting, switching or routing" data. In other words, it applies to the administrators of the connection, that operate the lower layers of the network, such as TCP/IP. There is no nothing in the law that provides that the neutrality would also reach the application layer. There are several reasons for this, as analyzed in this essay. The fact that the article 9 is included in a Chapter entitled "The provision of connection and Internet Applications" does not change this aspect. Thus, *it is understood that the network neutrality is directed specifically to the connection providers*, while the other provisions of this chapter as the "Protection of Records, the Personal Data and Private Communications", *also* go to application providers. From this point of view, the article 2, *caput*, of Decree nº 8.771/2016 goes further from the limits set by the law that it intended to regulate.

This article also suffers from a second vice. Thereof, *extending the network neutrality also to application providers, that operate exclusively in the top layer of the internet, conflicts with the constitutional principles of free enterprise and free competition*. As stated in the text, in this layer the rule is that every entrepreneur can benefit from competitive advantages, as a result of the innovations he has caused within the limits of legality. It is precisely the *temporary* privilege of exploitation of intellectual creations, exclusively (as in patents and software), which justifies and stimulates the innovation by encouraging investment in research and development areas. Stop this can cause serious side effects.

For these reasons, and in accordance with all the ideas developed throughout this text, it is reiterated that *the network neutrality focuses on the lower layers*, especially the TCP/IP protocols, preserving its full compatibility with any applications that already exist or that will exist. *In the application layer, differently, the rule is free competition*. Each developer can explore exclusively within the limits of law, the intellectual creations there were developed. Thus, *net neutrality is the prohibition to network*

administrators to manipulate the connection of users in order to discriminate the same type of data packets, based on their content, origin or destination, outside the legally permitted exceptions.

8 CONCLUSION

The internet is not the work of nature but the result of a human construction. It arose as a result of a unique historical moment, which brought together the military interest of the US Government, concerned with national security, and the participation of the academic elite of the country, centered on the ideal of freedom and sharing ideas. With these features it has consolidated and evolved, becoming one of the most important inventions of the recent history of mankind.

However, the internet has changed considerably in recent years. Some of its main features were replaced, to allow greater monitoring and control. The TCI/IP protocols, which were formerly neutrally used, now inspects the data packets, differentiating them by the source, destination or transmitted content. These changes opened the door for many forms of censorship and manipulation of users, which was not even imagined in the beginning of the internet.

Such changes have attracted attention from various fields of science, including the law. This paper has tried to contextualize, define and systematize the one that, in the author's view, is the main legal response to new challenges: network neutrality. Maybe with its correct application, it might be able to recover the balance of forces that exited in the origins of the Internet.

REFERENCES.

BAKER, Stephen. **Numerati.** Tradução: Ivo Korytowski. São Paulo: Saraiva, 2009.

BARLOW, John Perry. **A Declaration of the Independence of Cyberspace**. Avaiable at <https://projects.eff.org/~barlow/Declaration-Final.html>. Access on 28th December 2015.

BENKLER, Yochai. From consumers to users: Shifting the deeper structures of regulation toward sustainable commons and user access.

Federal Communications Law Journal. Washington: George Washington University Law School. v. 52, n. 03, p. 561-579. 2000.

CAPUTO, Victor. Mais da metade dos brasileiros são usuários da internet. **Caderno Tecnologia, Revista Exame.** Avaiable at <http://exame.abril.com.br/tecnologia/noticias/mais-da-metade-dos-brasileiros-sao-usuarios-da-internet>. Access on 7th April 2016.

CASSEB, Paulo Adib. Fundamentos Constitucionais do Marco Civil da Internet. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III:** Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. I.

CASTELLS, Manuel. **La Galaxia Internet**. Tradução: Raúl Quintana. Barcelona: Plaza & Janés Editores, 2001.

COMPARATO, Fábio Konder. Capitalismo e Poder Econômico. **Revista da Faculdade de Direito da UFMG**. Belo Horizonte, número especial: em memória do Professor Washington Peluso Albino de Souza, p. 167-195, 2013.

DE FRANCESCHI, Alberto; LEHMANN, Michael. Data as Tradeable Commodity and New Measures for their Protection. **The Italian Law Journal**. Napoli: Edizioni Scientifiche Italiane. v. 01, n. 01, p. 51-72, Mar. 2015.

FILHO, Eduardo Tomasevicius. O Marco Civil da Internet e as Liberdades de Mercado. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III:** Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. II.

FORGIONI, Paula Andrea; MIURA, Yuriko Rocha. O Princípio da Neutralidade de Rede e o Marco Civil da Internet no Brasil. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III:** Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. II.

GEIST, Michael. The Emergence of Net Neutrality Regulation in Canada: How Canada Developed a Consensus Policy on One of the Internet's Most Contentious Issues. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III**: Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. II.

HAFNER, Katie; LYON, Matthew. **Where Wizards Stay Up Late**: The origins of the internet. New York: Simon & Schuster, 1996.

KRISHNAN Ramayya; SMITH, Michael D.; TELANG, Rahul. The Economics of Peer-To-Peer Networks. **Journal of Information Technology Theory and Application**. Las Vegas: The University of Nevada. v. 05, n. 03, p. 01-24. 2003.

LEMOS, Ronaldo. Uma Breve História da Criação do Marco Civil. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III**: Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. I.

LENARD, Thomas M; MAY, Randolph J (Coord.). **Net Neutrality or Net Neutering**: Should Broadband Internet Services Be Regulated? New York: Springer, 2006.

LEONARDI, Marcel. Marco Civil da Internet e Proteção de Dados Pessoais. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III**: Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. I.

_____. **Responsabilidade Civil dos Provedores de Serviços de Internet**. São Paulo: Juarez de Oliveira, 2005.

LESSIG, Lawrence. **Code**: Version 2.0. New York: Basic Books, 2006.

_____.The Law of the Horse*:* What cyberlaw might teach**. Harvard Law Review.** New York: Aspen Law and Business, nº 113, p. 501-549, Dec. 1999.

MACIEL, Rafael Fernandes. A Requisição Judicial de Registro de Conexão e Aplicações no Marco Civil. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III**: Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. II.

MARTINS, Norberto Montani; DA SILVA, Pedro Miguel Bento Pereira. Funcionalidade dos sistemas financeiros e o financiamento a pequenas e médias empresas: o caso do *crowdfunding*. **Revista Economia Ensaios.** Uberlândia: EdUFU. v. 29, n. especial (Associação Keynesiana Brasileira), p. 25-56, Dez. 2014.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big Data**. New York: HMH, 2013.

OLIVEIRA, Raquel Diniz; PARENTONI, Leonardo. Uma Advertência sobre Interoperabilidade e o Artigo 154, Parágrafo Único, do CPC. **Revista Magister de Direito Civil e Processual Civil.** Porto Alegre: Magister, Ano IV, n.º 19, p. 51-73, jul./ago. 2007.

OPEN CONTENT. **Wikipedia**: The Free Encyclopedia. Entry: "Airbnb". Avaiable at <https://pt.wikipedia.org/wiki/Airbnb>. Access on 3rd April 2016.

_____. **Wikipedia**: The Free Encyclopedia. Entry: "Edward Snowden". Avaiable at <https://pt.wikipedia.org/wiki/Edward_Snowden>. Access on 4th April 2016.

_____. **Wikipedia**: The Free Encyclopedia. Entry: "Uber". Avaiable at <https://pt.wikipedia.org/wiki/Uber_%28empresa%29>. Access on 3rd April 2016.

PARENTONI, Leonardo. **Documento Eletrônico***:* Aplicação e Interpretação pelo Poder Judiciário. Curitiba: Juruá, 2007.

_____. SPAM: presente, passado e futuro. **Revista de Direito das Comunicações**. São Paulo: Revista dos Tribunais, ano 3, n. 5, p. 13-48, jan./jun. 2012.

RAMOS, Pedro Henrique Soares. O Marco Civil e a Importância da Neutralidade de Rede: Evidências Empíricas no Brasil. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III:** Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. II.

RANCHORDÁS, Sofia. Does Sharing Mean Caring? Innovation in the Sharing Economy. **Minnesota Journal of Law, Science & Technology**. Minneapolis: The University of Minnesota. v. 16, n. 01, p. 01-63, winter. 2015.

ROBERTS, Lawrence Gilman. The evolution of packet switching. **Proceedings of the IEEE**. New York: IEEE Foundation. v. 11, p. 1307-1313, Nov. 1978.

RODOTÀ, Stefano. **A Vida Na Sociedade da Vigilância.** Tradução: Maria Celina Bodin de Moraes. Rio de Janeiro: Renovar, 2008.

SALTZER, Jerome Howard; REED, D. P.; CLARK, David Dana. End-to-End Arguments in System Design. **ACM Transactions in Computer**

Systems. New York: ACM New York, v. 02, n. 04, p. 277-288, Nov. 1984.

SOLUM, Lawrence B.; CHUNG, Minn. The Layers Principle: Internet Architecture and the Law. **Notre Dame Law Review.** Notre Dame: University of Notre Dame Law School. v. 79, n. 03, p. 815-948, Jan. 2004.

TANENBAUM, Andrew S.; WETHERALL, David J. **Computer Networks**. 5th Ed. Boston: Pearson, 2011.

UNIÃO EUROPEIA. **Parlamento Europeu e Conselho da União Europeia**. Carta dos Direitos Fundamentais da União Europeia. Estrasburgo: 12 dez. 2007. Avaiable at <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:12012P>. Access on 4th April 2016.

UNITED STATES OF AMERICA. **The Internet Engineering Task Force – IETF**. Avaiable at <https://tools.ietf.org/html/rfc2460>. Access on 21 March 2016.

_____. **The Internet Engineering Task Force** – IETF. Avaiable at <https://tools.ietf.org/html/rfc791>. Access on 21st March 2016.

VAN SCHEWICK, Barbara. **Internet Architecture and Innovation**. Massachusetts: Mit Press, 2010.

VERGUEIRO, Luiz Fabricio Thaumaturgo. Marco Civil da Internet e Guerra Cibernética: Análise Comparativa à Luz do Manual de Talin Sobre os Princípios do Direito Internacional Aplicáveis à Guerra Cibernética. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III**: Marco Civil da Internet – Lei nº 12.965/2014. São Paulo: Quartier Latin, 2015. t. II.

WHITT, Richard S. A deference to protocol: Fashioning a three-dimensional public policy framework for the internet age. **Cardozo Arts & Entertainment Law Journal**. New York: Benjamin N. Cardozo School of Law. v. 31, n. 03, p. 689-768, Jul. 2013.

WU, Tim. Network Neutrality, Broadband Discrimination. **Journal of Telecommunications and High Technology Law.** Boulder: The University of Colorado, v. 02, n. 01, p. 141-176, Fall. 2003.

WU, Tim; YOO, Christopher S. Keeping the Internet Neutral? Tim Wu

and Christopher Yoo Debate. **Federal Communications Law Journal.** Bloomington: Indiana University Maurer School of Law. v. 59, n. 03, p. 575-592, June. 2007.

YOO, Christopher S. Protocol Layering and Internet Policy. **The University of Pennsylvania Law Review.** Philadelphia: The University of Pennsylvania. v. 161, n. 06, p. 1707-1771. 2013.

ZITTRAIN, Jonathan. **The Future of the Internet**: And how to stop it. London: Yale University Press, 2008.