From Snowden´s revelations to the Brazilian Legal Framework for the Internet: desecuritizing the cyberspace?

Tiago Vales[1]

It is known that cyberspace and information technologies have become almost essential to many of the activities of contemporary society. Mainly in the developed world, the daily practices have been linked and served much of the facilities offered by ITs, making cyberspace a kind of support for the productive and social activities. While it maximizes the ability of agents in varying degrees, these information tools also pose challenges to modern democracies. In this sense, the main challenge has been to create mechanisms respecting the established democratic rules in order to include cyberspace in a public governance, especially when it includes security issues with reflections on individual, government or financial fields, among others. This work intends to analyze the Brazilian behavior and interests on this issue of governance of cyberspace. By asking how the discourse concerning the internet and cyberspace helped Brazil to formalize its interests and policies domestic and internationally, this work argues that while Brazil started to formulate a set of rules of cyberspace that could be understood as the approbation of the "Legal Framework for the Internet", this same legal codes may contribute, at the same time, to a securitization of cyberspace or the agents participating on it as it shows no clear limits to the state or government actions on this field.

Key-words: Democracy, Cyberspace, Brazil, Internet, Security

1. Introduction

It is more than visible that the internet and a whole set of tools, devices, codes, etc. became a crucial part of contemporary social life. The flow of information, the easy ways to produce and to access was absorbed by the society in a relatively short period. From the beginning of the 90´s decade until the current years, Information Technologies (cell phones, personal computers, electronic devices in general) has increased in its capacity, efficiency, sophistication and variety of tasks. At the same time, it has been decreasing in price, the Information Technologies experimented a development, becoming more efficient, fast and

[1] Graduated in International Relations by the University of the State of São Paulo (UNESP) and master in History and Political Culture at the same university. Advanced Studies in Peace and International Security at the University of Coimbra (Portugal). Current PhD Candidate in International Relations – International Politics and Conflict Resolution at the University of Coimbra, Portugal. The present paper is part of a project funded by the Fundação para a Ciência e Tecnologia (FCT) in Portugal.

present in daily activities, from checking messages in personal cellphones to the movement of large sums of money around the world. Money that incidentally exists only electronically (Lévy, 2003; Castells, 2005).

More than becoming part of almost every activity, the access to Information Technologies and the use and interactions become synonymous of development. In this sense, many politics of developing information technologies in order to decrease even more the prices has been implemented at the same time many initiatives of making the internet available to people in underdeveloped countries has been encouraged. For example, Information companies such as Google or Facebook have implemented measures to provide access to remote parts of Africa (Thielman, 2015). The justification for these actions remains on the idea of emancipation of the population located in places that lacks or have none means of communication. In this sense, non-profit organizations also joined this issue and have their own politics. The World Telecommunication Union, for example, dedicated some meetings and conferences to the overcome what is known by digital divide[2] (ITU, 2016: online).

Resuming, the technological development, mainly in the Information Technologies represents a major sector of the contemporary globalized and interdependent economy (Albert & Papp, 1997: ii). Those technologies and its growing availability reveals the advent of what Castells calls the IT Paradigm. Considering those elements are an important part of social life (Lévy, 2003), it is possible to observe what has been understood by the ´information society´ (Cardoso, 1998; Castells, 2003).

Thus, it is noted that the evolution of IT enabled a new free from state boundaries globalized public space, for now, without apparent control by any State or other entity. This space, in particular the internet and its tools, can be defined as cyberspace. This space has pervaded social relations allowing different actors to meet and develop their interests in a large and dynamic network of contacts and possibilities. According to Bells´ (2004) definition,

> Cyberspace is a term used to describe the space created through the confluence of electronic communications networks such as the Internet which enables computer mediated communication (CMC) between any number of people who may be geographically dispersed around the globe.

Among the challenges posed by the rising of cyberspace as a new element of contemporary society, a special attention must be given to security issues. Many of the existent threats to the normal conduct of social life in several areas: terrorism, theft of data, access control, and operation of infrastructure, hacking attacks, cyber warfare (Lewis, 2002). Evaluating such threats or challenges, States and multilateral organizations have taken certain measures or policies to promote cyber security threats as well as to prevent or promote the governance of internet in both domestic and international level. One of the most visible initiatives in this sense was sponsored by the North Atlantic Treaty Organization (NATO) published as the Tallinn

[2] As defined by Internet World Stats, Digital Divide, digital split or digital gap refers to the amount of information between those people who have access to Internet and those who do not have. (Internet World Stats, 2016: online).

Manual in symbolic allusion to the place where it was designed and developments related to cybersecurity involving Estonia in 2007[3].

This work will look to this attempt of promote governance in internet in the particular case of Brazil. The South American country has developed a Legal Framework, called the Civil Rights Framework for Internet (CFI), to set the role of the many actors in internet and regulate their rights and responsibilities. It includes the regular users, private companies, non-profit organizations, civil associations and the Brazilian State. Beyond that, Brazil started a campaign in international forums in order to try to promote the governance of internet in a multilateral agreement under the egis of international organizations.

Despite the Brazilian president, Dilma Rousseff, has defined CRFI as the world´s most advanced law in defense of internet (Palácio do Planalto, 2014: online), it comes with some problems. Some of these issues concerns the role of the State, since it is not specific enough, for one side, and the role of the state and its institutions are regulated by some other legal documents, specially when it comes to security and defense issues, for other.

This work intends to analyze, the role of Brazilian initiatives for the governance of the cyberspace under the light of securitization theories,. This paper argues that while Brazil desecuritizes the cyberspace through the "Civil Framework for the Internet" by answering concerns regarding the roles of different actors that deal with the cyberspace, at the same time the Legal Framework may contribute to a re-securitization of the cyberspace, by not clearly limiting State action on this field.

To develop this argument, this text will be divided in three main parts. Considering the main theoretical frameworks for this paper remains on the Securituization theories, the first part is dedicated to a brief summary of this theory. Since the establishments of the Legal Framework for Internet in Brazil is understood here as an ongoing desecuritization process, this part also addresses the general concepts of this aspect of the theory. Turning into a more specific approach, the following parts will be directed to explore the availability and the usage of internet in Brazil and the analysis of the Civil Framework for the Internet focused on the role of the state in this issue.

2. Securitization and desecuritization

The issues concerning security are generally at the core of the Estate purposes. Nevertheless, the decision concerning what is priority among the security issues is still a complex process. The decision makers have a broad scope into consideration to stablish their policies and measures. The context involving the decision on what is to be priority security issues permeates a several elements, like personal evaluations, interests from groups or personal, the personal understanding of the decision makers, the discourse of different actors. The discourse is one

[3] In 2007 a series of cyberattacks were perpetrated against the Estonia cyber infrastructure. It put down all the online services of the country. Considering Estonia is one of the most "cyberized" countries in the word and a important part of the services are made online, it represented a grave issue for Estonians. More than that, the suspect that the Russian hackers with support of the government coordinated the attacks. As the attacks are considered the first act of war in cyberspace, many actors and researchers from political science to informatics have dedicated their works on this episode. As for political field Hansen and Nissembaum (2009), Valeriano and Maness (2015),

fundamental piece of this whole as it is used to justify measures to be taken, to stablish what is really a security concern and to pint who are the actor responsible to take the adequate policy.

The systematization or theorization concerning this decision process is set by the Theory of Securitization, originally thought under the Copenhagen School of Securitization and complemented by other scholars. Having approached the relevance of the cyberspace issues in general at the introduction, this part will focus on the Securitization and Desecuritization and a brief literature review approaching the mentioned theories with the concerning of security for cyberspace.

As originally argues by the theorist of the Copenhagen School, to become a security priority an issue passes through some steps that could culminate in a securitized theme. This process is mentioned as the "securitizing move". As Buzan et al. defines, it is a "a discourse that takes the form of presenting something as an existential threat to a referent object" (1998: 25). This discourse is set to convince a determined audience of the necessity to adopt special measures to protect determined and alleged threated element (Taurec, 2006), or, the referent object, that is open to any element which existence or operation is considered essential for a determined audience. (Buzan et al. 1998: 25). This securitization move can be seen as the first step of the securitization process.

The discourses or speeches remain as a central element of the securitization process. According to Weaver, is through the discourses that a threat can be addressed and thus convince the functional actor to take the necessary measures to protect the referent object. The discourse labelling something as a security issue while identifying an existential threat qualifies a special kind of politics to be adopted as a legitimate urgent measure by the decision makers (Buzan et al. 1998: 23). As explained by Weaver (2012) "a designation of the threat as existential justifies the use of extraordinary measures to handle it. The evocation of security opens the way of the state to take special power". The referent object is something central to a securitization process as it has to be something that deserves protection, otherwise the cease of its existence will jeopardize seriously something that is truly important to a society or a group.

Beyond that, in the speech acts the securitizing actor targets the functional actor, or the one (person, representative, institution, etc.) who are able to take measures to deal with the threat and protect the referent object. The functional actor has to be the one who are involved in authority to make decisions.

Resuming, as argues by the Securitization Theory, the security issues are basically a successful speech provided by a securitizing actor. This actor, or group of actors targets determined audience (citizens, decision makers, representatives, who has the authority to adopt policies) and justify the use of special measures to protect or to make the existence of the referent object secure which is essential to this audience. In this case, security become a social-constructed issue and not a pre-stablished concern (Balzacq, 2005). As explained by Buzan,

> Security is thus a self-referential practice, because it is in this practice that the issue becomes a security issue – not necessarily a real existential threat exists but because the issue is presented as such threat" […] "when a securitizing actor uses a rethoric of existential threat and thereby takes an issue out of what under those conditions is "normal politics", we have a case of securitization". (Buzan et al. 1998: 24).

The problem of the securitization process is precisely its success. As argued by Weaver (2005), while the securitization process addresses special measures to face threats, it automatically brings the security issues out of the normal conduct. It provokes, at the first moment, a high politicization of the discussions and, at the end, brings the politicized theme to an exceptional policy field.

According to Buzan at al. (1998) the securitization is something to be avoided, because it provokes distortions on the normal conduct and management of security issues. As a goal, Weaver (1995) proposes the opposite movement where a desecuritization process will be able to bring the security discussions and decisions to the normal rules.

As in the securitization processes, it is possible to note the elements of the desecuritization processes. Notwithstanding, the desecuritization is a processes that has to be more accurately analyzed mainly because the "desecuritization move" may not be as clear as the securitization. The securitization can be presented in a more specific ways and the role of the actors, if there is any, may not present the same characteristics of the ones in the securitization processes. Resuming, the desecuritization cannot always be seen as the symmetric opposition of the securitization.

Accoding to Weaver (1995, 59 – 60) the desecuritization must be the main goal in a securitized context. The actors must search for the demobilization of the special measures that characterizes a securitized process and bring back the securitized issue to be treated in the normal realm of the politics. As Weaver points, it is necessary to transform "treats into challenges and security into politics" (Weaver, 1995: 60).

Despite the desecuritization is the main goal, this aspect is undertheorized and little explored in the literature dedicated to the theories of securitization. The author, however, points three ways that desecuritization could take place.

The first is to avoid the discourse that formalizes a securitization. According to Biba (2013: 10) it could be understood as a non-securitization process. This idea suggests that the desecuritization doesn´t depend necessary to a securitized context and could be conscientiously applied as a policy of prevention or in an ongoing securitization process.

The second strategy for desecuritization involves the management of the securitized issues. It can happen in many ways, since the establishments of rules to deal with this situations and similar ones, the cease of the feeling of threat, among others. This strategy must considerer important aspects and be very clear to not submit this issues in a cyclical process, making a kind of (re)securitization possible.

The third is the one that most closely matches the contrary movement of securitization. It is implemented by the contrary discourse of securitization, directed to bring the securitizes issue to the normal rules. As Roe suggest, this movement can be identified as a transformation movement (Roe, 2004).

All of these aspects meets some particularities while applied to a determined context and sometimes the combination of strategies can be seen. It seems to be the case of Brazil, as it will be explored in the following pages.

The security and cyberspace has been analyzed through several theoretical lens, from the National Security studies, as in Reveron (2012), Giacomello (2014), and different approaches in Eriksson and Giacomello (2007), to the different implications of the raising of cyberspace for International Relations and for the State, as in Choucri (2014). Also, the role of

the State dealing with this relatively new environment is explored by Nye (2011) and Naim (2014). Notwithstanding, Castells (2005), in a broad and sociological approach, treats the cyberspace as a new age with implications for the social configurations in general.

The Securitization approach for cyberspace is also explored by the security studies literature, including a brief mention by the original formulators of the theory. As Buzan et al. (1998: 163 – 164) mentioning the work of Nierop and Der Derian, points still in the early 90´s, that the rise of cyberspace will promote such a dynamic relations that could become a subject of security, due the globalization process.

This issue of cyberspace linked to security also appears in Buzan and Hensen (2009: 228) as a matter of international security manly after the 2011 attacks in United States. According to the authors, the particularity of the securitization of the cyberspace is the permeability to several sectors but it does not constitute a particular sector itself. As the theory suggests, there are five main sectos in security issues: Societal security, Economic security, Environmental security, Political security and the traditional Military security. The securitization of cyberspace dialogues or has implications in more than one sector at the same time.

This issue was deepened by Hensen and Nissembaum (2009: 1167). The authors suggested that the securitization of cyberspace happens in three specific categories: a) Hypersecuritization: generally supported by a hype involving the security issues, claiming exceptional measures, b) everyday security practices: connecting the cybersecurity issues and threats to daily life; c) technifications, limiting the security in the cyberspace to a high level of technical experts, bringing the decisions out of the political realm, as said by the authors, “if cyber security is so crucial it should not be left to amateurs”.

It is also important to stress the military dimension of the securitization of cyberspace. Some countries as China, according to Ball (2011) points cyberspace and military activities or expertize on that must set another domain among the traditional ones. Some authors have already analyzed this dimension. Cavelty (2012) at some point understands that while cyberspace can be seen as one aspect of national security issue it could be applied to military matters, since it could become a priority and a sensible point of reflection for national interests and protection. As the complexity of the attacks in cyberspace by hackers, the sophistication of cybercrime increases this views are reinforced. Some cases are clearly visible, as some countries have military divisions in charge of the protection of cyber activities considered strategic for the governments.

This military dimension also meets the cyberspace specifically in this securitization approache. As Hare (2010) elaborates, a military aspect, conjugated with the social-cultural cohesion of a country can be a ruler to measure or provide a set of elements to characterize and compare the securitization of cyberspace in different countries. According to his theoretical model, weak states (in military terms) with poor or deficient cultural cohesion are more likely to securitize cyberspace than the stronger ones. However, this model, despite of presenting interesting elements to be tested as a theory, was not applied to any concrete situation.

There are few mentions concerning the desecuritization of cyberspace. Not only because this specificity of cyberspace configures a theme to be explored but this theoretical approach in general needs to be developed both theoretical and empirical aspects. Among the few mentions, Giacomello (2007) suggests that some governments, namely France and United States, persuaded by the private sector are regularizing the use of instruments as encryption by civil consumers instead of keeping it restricted to military issues. An interpretation is possible

here. As the desecuritization passes through a process of regularization by the state institutions and initiatives, there is a suggestion that this move can be a type of “desecuritization move” that could bring back a restricted instrument (in this case very specific as the encryption) to the normal ways of conduction of rules and uses.

In order to approach Brazilian initiatives concerning the cyberspace, it is useful to have a look at the Brazilian cyberspace reality. The next part will present a brief background on how representative and important the cyberspace and the use of its instrument is for the Brazilian users in general, including the government.

3. Brazil´s policies for cyberspace: from users to security tools.

Brazil has been witnessing a steady increase in its internet usage since the early 90s. Just like the rest of the world, the internet in Brazil was first restricted to small groups of governmental agencies and academic research centers. While the activities on the Internet crossed the boundaries of academic and scientific fields to become a business issue, the infrastructure of connections, hardware were ameliorated, the quality of connections was increased and the prices were reduced. As a result, the number of users have also increased forcing the government and companies to widen their services to include other fields and offer online solutions to attract more customers.

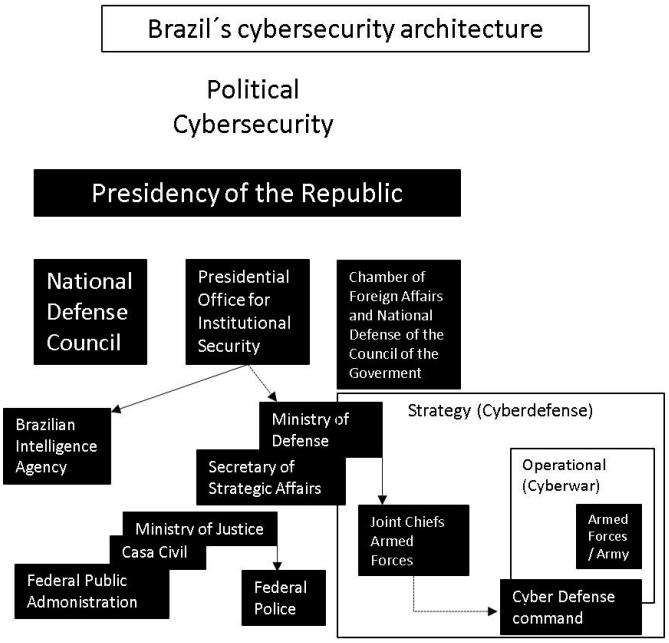
Nowadays, the internet and its services and tools encompass roughly 140 million users, or around 66% of the total Brazilian population (Internet Live Stats, 2016). In economic terms, these users are responsible to transferring more than 20 billion dollars (Statista, 2016). Furthermore, important activities like Internet Banking, social networks, e-governance services, are among most developed and diffused activities in Brazil. It's because of activities as such, Brazil is considered to be the most “cyberized” nation in Latin America and can also be considered as the one of most cyber-inclusive nations in the world. There are some big gaps however, that need to be addressed by the politics of inclusion already in course (Pedrozo, 2013).

Since cyberspace occupies an influential and relatively large field in Brazil, the country has established institutions in order to address internet related issues, from the regulation of the role of users and service providers, to the most complex security matters involving military and strategic decisions at the state level and according to Diniz et al (2014), many of the entities are linked to the technical management of systems

The implementations of policies, elaboration of legal or normative guidelines, were submitted to a small but very important part of institutions in a political hierarchy. The President of the Republic is the head of the organization of this field that includes governmental institutions like the Brazilian Intelligence Agency (Abin), the Ministry of Defense, the National Defense Council, the Armed Forces and the Join Chief of Staff and the Federal Policy. Correspondingly, the country can conjoin many important institutions that handle national security issues

Over and above, Brazil has recently published its security strategy in two main documents, the National Strategy Defense (2008) and the White Paper to Guide Future Defense Priorities (2012). What concerns cyberspace policies, the country published the Green Book on Brazil´s Cybersecurity in 2010 (Presidência da República, 2010) but, the most important

document in this field is the CFI which was approved in 2014 and regulated by the former president Dilma Rousseff in 2016. These hierarchical relations among the institutions can be better visualized in Diniz et al. (2014). The authors offer a visual scheme of the Brazilian main institutions and their relations with cyber security and the defense structure:



Source: Adapted from Diniz at al (2014).

3.1 The Security discourse and the Brazilian Civil Framework for the Internet

Beyond the security concerns, cyberspace has become an object of internal and foreign policy The security discourse that in this view is homogenous with the behavior of the Brazilian authorities to the Securitization process - explored in the first part of this paper - took place before the approbation of the Civil Framework for the Internet (CFI)[4].

The importance of cyberspace as a strategic security sector and its implications to foreign relations, was clearly revealed by the former Brazilian Minister of defense in 2013, Celso Amorim, when he defended a more active policy for the development of cyber capacity in order for Brazil to be able to play an adequate role in the international scenario along with other powers that have more capacity. As Amorim (2013: 292), was the former Minister of Foreign Affairs, warns:

> "Se nada for feito, o risco que corremos, diante da escalada contínua de arsenais ofensivos [armamentos cibernéticos] é

[4] It is important to emphasize that the CFI was proposed as a project of law by the Presidency of the Republic, in 2011, already under the Rousseff´s mandate. This initiative precedes any denounces of espionage or security issues for cyberspace bade public. Of course, there were some discussions about the implications of this set of rules and some polemics, according to some news agencies as in Coutinho (2012) and specialized pages, like in Grossmann (2012).

> que, em algum momento, venha a ser proposto um tratado que congele as disparidades do poder militar cibernético" [5]

This discursive connection between security and cyberspace was unraveled when this issue reached the public opinion in 2013. In this very year, the former employee of the American National Security Agency (NSA), Edward Snowden, denounced a practice of cyber espionage on many international leaders and high authorities in several countries, sponsored by the American government (Greenwald, 2015).

In what concerns Brazil, the American agency, scandal, hacked some e-mail accounts of the former Brazilian president Dilma Rousseff as well as e-mails of high ranked government officials, including directors from Petrobras, the Brazilian State oil company (Harding, 2014). The Brazilian press emphasized on this event, as it became a very sensitive international issue.

As a result, this episode had many implications for the political fields, at both international and domestic levels. In terms of foreign relations, Snowden´s revelations provoked a diplomatic dispute between Brazil and the United States and forced Brazil to officially convey its discontent. The bilateral relations witnessed a huge setback but not to the extent of cutting diplomatic ties., this event. Rousseff cancelled (Monteiro, 2013) a scheduled visit to Washington. Furthermore, the Brazilian Minister of Foreign Affairs, the Itamaraty, issued a note addressing some important elements, classifying the act of espionage perpetrated by the American government as a serious attempt against the national sovereignty and to individual rights:

> "As práticas ilegais de interceptação das comunicações e dados de cidadãos, empresas e membros do governo brasileiro constituem fato grave, atentatório à soberania nacional e aos direitos individuais, e incompatível com a convivência democrática entre países amigos" [6] (Palácio do Planalto, 2013)

Rousseff used this discourse to further bolster her arguments at the 68th Section of General Assembly of United Nations. While she conveyed Brazil's discontent with the practices sponsored by the U.S government, she specified some elements and proposals to be discussed at the International Initiative Towards the Protection of Privacy in Internet. As she pointed:

> "Estamos, senhor presidente, diante de um caso grave de violação dos direitos humanos e das liberdades civis; da invasão e captura de informações sigilosas relativas as atividades empresariais e, sobretudo, de desrespeito à soberania nacional do meu país. Fizemos saber ao governo norte-americano nosso

[5] If nothing is done, the risk we run, given the continued escalation of offensive arsenals [cyber weapons] is that, at some point, will be proposed a treaty to freeze disparities cyber military power. (Free translation)

[6] Illegal practices of interception of communications and data from citizens, companies and Brazilian government officials are serious issue and a threat to the national sovereignty and to individual rights, and inconsistent with the democratic coexistence between friendly countries. (Free translation)

> protesto, exigindo explicações, desculpas e garantias de que tais procedimentos não se repetirão" [7] (Palácio do Planalto, 2013)

From a domestic standpoint, there was already an ongoing discussion about the role of actors (companies, State, users) in internet. In fact, the espionage scandal has pulled this discussion towards the approbation of what became known as the Civil Framework of the Internet (Palácio do Planalto, 2014). Although it wasn't directly associated with the Snowden case and was actually criticized by some civil sectors, the Civil Framework for Internet was approved by the Brazilian congress in 2014.

Consequently, the approbation of the Civil Framework for the Internet wasn´t unanimous, although the law doesn't comprise an article that explicitily tackles the issue of defending the country against espionage, , that issue itself was the main topic of discussion for some parliamentarians:

> As recentes denúncias de espionagem contra o Brasil pelos Estados Unidos, conforme documentos mostrados pelo ex-analista da Agência Nacional de Segurança (NSA) Edward Snowden, tornaram ainda mais urgente a aprovação de um marco regulatório para a Internet no Brasil. Sua aprovação não resolverá o problema da espionagem, mas é um passo importante para proteger a privacidade da sociedade da cyberespionagem, bem como para promover a inovação e o desenvolvimento social e econômico do Brasil, e impulsionar uma Internet mais igualitária e justa.[8] (Guimarães, 2013)

As this approach for security constituted some valorous argument to the approbation of the CFI which could be interpreted as a securitization move, but not necessarily a complete securitization process, the document itself doesn´t extend to security issues.

Despite the avoidance of the securitization discourse, some actors choose to raise some security issues. Their alleged ideas suggest the implementation of tools to avoid the securitization in an attempt to stablish or create ways to deal with similar situations. It is possible to link this movement to the aforementioned way of securitization, namely, the management of securitized issue. In this case, it is important to observe, there isn´t a proper securitized issue.

---

[7] We are, Mr. President, faced with a serious case of violation of human rights and civil liberties; the invasion and capture sensitive information concerning the business activities and, above all, a disrespect for national sovereignty of my country. We made known our protest to US government, demanding explanations, apologies and assurances that such procedures will not be repeated (Free Translation)

[8] Recent spy allegations against Brazil by the United States, according to documents shown by former analyst at the National Security Agency (NSA) Edward Snowden, made even more urgent the approval of a regulatory framework for the Internet in Brazil. Approval will not solve the problem of espionage, but it is an important step to protect the privacy of society form cyberespionage, and to promote innovation and social and economic development of Brazil, and promote a more just and egalitarian Internet. (Free Translation)

A contrary movement of securitization can also be observed as the alleged intentions for the approval of the CFI were made towards a more democratic cyberspace. These intentions will bringing some issues to a normal set of rules to be applied in their normal juridical aspects.

The approved set of rules was highly castigated even after two years from its approbation and was far from being unanimous. In fact, the final document lacked articles concerning some aspects of cyberspace , including the role of the public power in security and defense. The next part will focus on the main aspects of the Legal Framework for the Internet in accordance of what this paper proposes.

3.2 Considerations on the Brazilian Civil Framework for the Internet

The Brazilian CFI, or law No. 12.965, April 23rd 2014 is dedicated, as the text says, to the establishment of "the principles, guarantees, rights and obligations for the use of the Internet in Brazil" [9] (Brasil, 2014). The intentions, disposed on the preliminary provisions (Chapter one) is to embrace all the aspects of the use of internet, recognizing its global amplitude and mentioning some important aspects related to the protection of data and the neutrality of the networks.

The document defines the elements of internet upon which the law will pe applied r. In doing that, the Brazilian State determines what is understood by Internet and its comprehensiveness:

> "[A internet é o] sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes"[10]

What is perplexing in this case is that while CFI recognizes the borderless characteristic of the internet since, (as the definition states that the internet structure is set in a world scale), these set of laws are actually inapplicable in Brazil because they affect on the Brazilian sovereignty.

Additionally, the CFI is introduced as a complementary law to the existent one and presents a juridical framework, from International treaties to domestic criminal settings. Although it implies that the Framework is specific for internet usage, including the role of the States and the Union, it does not determine the limits of each public actor in case of a conflict of interests. In this case of the extension of the internet, given its borderless characteristics it represents an ongoing debate, not only in the Brazilian case but in the general attempt of the governance of internet.

---

[9] The final text of the law can be found in <https://www.publicknowledge.org/assets/uploads/documents/APPROVED-MARCO-CIVIL-MAY-2014.pdf> both in Portuguese and English. There is no official translation to English.

[10] [The Internet is] the system consisting of the set of logical protocols, structured on a global scale for public and unrestricted use, in order to enable communication of data between terminals, through different networks. (Free translation)

Chapter 4 of the Framework is dedicated to scrutinizing the actions of the public power. This chapter delves into the liberties and warranties of the development and improvement of the internet's infrastructure, the promotion of the governance and transparency of the official information of private, public and academic sectors. The security issues are left for those who have the technical capacity , namely, at the state level, the Cyber Command of the Army who shares this responsibility with private sector.

Considering the securitization scheme an aspect of the technical responsibilities - as argued by Hensen and Nissembaum (2009)- this very aspect matches the securitization doors of andpresents the “technification” as an argument to prompt it to a 'special' field of decisions.

The role of the state and security agents in case of an alleged threat, such as espionage, theft of financial data or even theft of industrial information will be a military and strategic decision and not necessarily a public discussion.

Although claiming to be comprehensive, the Framework is very open to many interpretations, as it presents general aspects of the use of internet and ascribes the private sector as the main actor responsible for safeguarding the data. What is intriguing in this context, is the possibility for the private sector to be considered as the main actor that can declassify the internet service for the uttermost users in Brazil.

4. Final Words

In the way it is presented, the CFI of internet could be a interesting tool concerning the defense of the customers or users of the internet in Brazil. At the same time, the document seems to be vague when it comes to security issues. Despite some security issues were evoked to give support the approbation of the Framework this very issues were not fully or enough contemplated on the final text. On the contrary, the final text only mention some generic security issues and not even mention the institutions and organs responsible for this subject.

The evocation of some security aspects when the discussions for the approbation took place suggests there were a beginning of a securitization process. Some discourses of the favorable parts and other authorities interested on the implementation of politics for the cyberspace pointed some issues like the right of privacy, the national sovereign, the national interests and the necessity to implement measures to face the international concurrence on the cyber capabilities.

In fact, the issue of cyberspace were not fully securitized, despite the technical issues are delegated to a military organ and kept as a high state institutions policy. But the securitization discourse were useful to bring the public opinion, the press, etc. to a politicization of this issue, further amplified by the denounces performed by Edward Snowden.

Despite the allegation the CFI for the Internet is considered by supporters as one of the most advanced legal settings concerning this issue of rights and duties in cyberspace, it didn´t prevent some controversial decisions. There is some In Brazil, as the prohibition of WhatsApp for allegedly not cooperating with justice, and the prison of the Latin American Facebook CEO for the same reason (Connors and Jelmeyer, 2015; Watts, 2015)

For being generic and focused on the business issues more than in the State duties, the CFI leaves some open doors for the securitization of the cyberspace in Brazil, depending on

the interests of the State or the government. Beyond that, the security issues of cyberspace in Brazil, as in many other countries appear as a technical issue under the military responsibility, what matches the technification argument for the securitization of cyberspace.

It seems that to keep the cyberspace desecuritized, there is a necessity to keep this issue on the politics, politicized and discussed not only by the technical side, but on the implications it have on the society in general.

5. References

Albert, David. Papp, Daniel (1997) The information age: an anthology on its impact and Consequences. CCRP Publication Series. Available in: http://www.dodccrp.org/files/Alberts_Anthology_I.pdf

Amorim, Celso (2013) "Segurança Internacional: Novos desafios para o Brasil". Contexto Internacional. 35(1) 287 – 311.

Balzacq, Thierry (2005) "Three faces of securitization", European Journal of International Relations June 2005 11(2) 171-201

Ball, Desmond (2011) "China´s Cyberspace capabilities". Security Challenges, Vol. 7, No. 2 (Winter 2011), pp. 81-103.

Bell, David (2004) Cyberculture: the key Concepts. New York. Routledge

Biba, Sebastian (2013) Desecuritization in China´s Behavior Towards its transboundary rivers: the Mekong River, The Brahmaputra River, and the Irtysh and Ili Rivers. Journal of Contemporary China, 23 (85) 21-43

Buzan, Barry et al. (1998) Security: a New framework for Analysis. Boulder: Lynne Rienner

Cardoso, G (1998) "Para uma sociologia do cyberespaço: comunidades virtuais em português" . Oeiras: Celta Editora.

Castells, M. (2005) A Sociedade em rede. Lisboa: Fundação Calouste Gulbenkian

Cavelty, M. The militarisation of cyber security as a source of global tension. In: MÖCKLI, D. Strategic trends 2012: key developments in global affairs. Zurich: 28 Center for Security Studies (CSS), 2012.

Choucri, Nazli (2014) Cyberpolitics in International Relations. Cambridge. MIT Press.

Coutinho, Katherine (2012) "Regulação do Marco civil na internet ainda precisa de ajustes". Available in: http://g1.globo.com/pernambuco/noticia/2012/07/regulamentacao-do-marco-civil-na-internet-ainda-precisa-de-ajustes.html

Connors, Will; Jelmeyer, Rogério (2015) "Brazilian Judge lifts ban on Facebook and WhatsApp. The Wall Street Journal. Tech. Available in: http://www.wsj.com/articles/brazil-court-suspends-facebooks-whatsapp-for-48-hours-1450348131

Diniz, Gustavo et al. (2014) Deconstructing Cyber Security in Brazil: threats and Responses. Igarape Publication. Strategic paper. December 2014. Available in: https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf

Giacomello, Giampiero (2014) Security in Cyberspace: Targeting Nations, Infrastructures, Individuals. London: Bloomsbury

Giacomello, Giampiero; Eriksson, Johan (2007) International Relations and Security in the Digital Age. New York: Routledge.

Greenwald, Gleen (2014) No place to hide: Edward Snowden, the NSA, and the U.S. Surveillance State. New York: Metropolitan Books

Grosmans, Luis (2012) "Confrontos do marco civil: neutralidade da rede". Available in: http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=32413&sid=4

Guimarães, José (2013) "Urgência do Marco Civil da Internet" Available in: http://www.ptnacamara.org.br/index.php/inicio/artigos/item/16035-a-urgencia-do-marco-civil-da-internet-artigo-do-deputado-jose-guimaraes.

Hansen, Lene; Nissenbaum, Helen (2009) Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly, 53, 1155–1175

Hare, Forrest (2010) "The cyber threat to National Security: why can´t we agree?" Conference on Cyber Conflict Preceedings 2010. Available in: https://ccdcoe.org/sites/default/files/multimedia/pdf/Hare%20-%20The%20Cyber%20Threat%20to%20National%20Security%20Why%20Cant%20We%20Agree.pdf.

Harding, Luke (2014) The Snowden files. New York: Vintage Books.

Internet World Stats (2016) "The digital divide, ICT, and Broadband Internet". Available in http://www.internetworldstats.com/links10.htm. Access on February 2016.

Internet Live Stats (2016) "Brazil Internet Users(2016)". Internet Live Stats, available in: http://www.internetlivestats.com/internet-users-by-country/brazil.

Lévy, Pierre (2003) Cyberdemocracia. Lisboa. Instituto Piaget.

Lewis, James (2002) "Assessing the risks of cyber terrorism, cyberwar, and other cyber threats. Center of Strategic and International Studies. Available in: https://www.ciaonet.org/attachments/5845/uploads

Monteiro, Tania (2013) "Dilma Cancela viagem aos EUA". O Estado de S.Paulo. Availbla in: http://politica.estadao.com.br/noticias/geral,dilma-cancela-viagem-aos-eua,1075730

Naim, Moises (2014) The end of the power. New York. Basic Books.

Nye, Joseph (2011) The future of the power. New York. Public Affairs

Palácio do Planalto (2013) "Visita ofocial aos Estados Unidos será adiada". Available in: http://blog.planalto.gov.br/visita-oficial-aos-estados-unidos-sera-adiada/.

Palácio do Planalto (2013b) “Discurso da Presidenta da República, Dilma Rousseff, na abertura do Debate Geral da 68ª Assembleia-Geral das Nações Unidas – Nova Iorque/EUA. Available in: http://www2.planalto.gov.br/acompanhe-o-planalto/discursos/discursos-da-presidenta/discurso-da-presidenta-da-republica-dilma-rousseff-na-abertura-do-debate-geral-da-68a-assembleia-geral-das-nacoes-unidas-nova-iorque-eua

Palácio do Planalto (2014) “Dilma: Marco civil é a legislação mais avançada no mundo e nos coloca na vanguarda da proteção dos usuários da Internet”. Availabe in: http://blog.planalto.gov.br/dilma-marco-civil-e-a-legislacao-mais-avancada-no-mundo-e-nos-coloca-na-vanguarda-na-protecao-dos-usuarios-da-internet. Access on February 2016.

Palácio do Planalto (2014b) “LEI Nº 12.965, DE 23 DE ABRIL DE 2014.” Marco Civil da Internet. Available in: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

Palácio do Planalto (2010) Livro verde da Segurança Cibernética no Brasil. Available in: http://dsic.planalto.gov.br/documentos/publicacoes/1_Livro_Verde_SEG_ CIBER.pdf

Pedrozo, Sueila (2013) “New Media use in Brazil: digital inclusion or digital divide”. *Online journal of Communication and Media Technologies,* 3(1).

Reveron, Dereck (2012) Cyberspace and National Security: Threats opportunities, and power in a Virtual World. Washington: Georgetown University Press

Roe, Paul (2204) “Securitization and Minory rights: conditions of desecuritization”. Security Dialogue, 35(3), 279-294

Statista (2016) “Retail e-commerce sales in Brazil from 2014 to 2019”. Available in: http://www.statista.com/statistics/289746/brazil-retail-e-commerce-sales/.

Taurec, Rita (2006) “Securitization theory and securitization studies”. Journal of International Relations and Development, 9 (1), 53 – 61.

Thielman, Sam (2015) *Facebook satellite to beam internet to remote regions in Africa*. Tech. The Guardian. Available in: http://www.theguardian.com/technology/2015/oct/05/facebook-mark-zuckerberg-internet-access-africa. Access February 2016.

ITU (2016) Connect the world. Online. Availabe in: http://www.itu.int/en/ITU-D/Conferences/connect/Pages/default.aspx. Access on February 2016.

Valeriano, Brandon; Maness, Ryan (2015) Cyberwar versus Cyber Realities. Oxford: Oxford University Press

Watts, Johnatan (2016) “Brazilian Police arrest Facebook´s Latin America Vice-President. The Guardian. Tech. Available in: https://www.theguardian.com/technology/2016/mar/01/brazil-police-arrest-facebook-latin-america-vice-president-diego-dzodan.

Weaver, Ole (1995) “Securitization and desecuritization”. In Lipschutz, Ronnie (1995) On security. New York: Columbia

Weaver, Ole (2012) “Aberystwith, Paris and Copenhagen. “The Europeanness of new “schools” of security theory in an American Field”. In Tickner, A & Blaney, D. (eds). Thinking International Relation Differently. New York: Routledge