Is there a way to desecuritise cyberspace? How Brazil’s Legal Framework for the Internet could have done that

https://doi.org/10.22151/ELA.4.2.5

Tiago Vales
PhD Candidate in International Relations – International Politics and Conflict Resolution at the University of Coimbra, Portugal.
tpvales@gmail.com

Joe Abdul Sater
PhD Candidate in Sociology at the University of Coimbra, Portugal
joeabdulsater@hotmail.com

Abstract
Cyberspace and information technologies (ITs) have become essential to many of the activities of contemporary society. Mainly in the developed world, the daily practices have been linked to and served much of the facilities offered by ITs, making cyberspace a kind of support for the productive and social activities. While they maximise the ability of agents, these information tools also pose challenges to modern democracies. By asking how the discourse on the internet and cyberspace helped Brazil formalise its interests and policies domestically and abroad, this work argues that while Brazil started to formulate a set of rules for the cyberspace that could be understood as the approbation of the ‘Legal Framework for the Internet’, such legal code may contribute, at the same time, to a ‘securitisation’ of cyberspace.

Key-words: Democracy, Cyberspace, Brazil, Internet, Security, Legal Framework, Securitisation, Desecuritisation
Introduction

It is more than visible that the internet and a whole set of tools, devices, codes, among others, became a crucial part of contemporary social life. The flow of information, the ways to produce and access it were absorbed by the society in a relatively short period. From the beginning of the 90’s until nowadays, Information Technologies (cell phones, personal computers and electronic devices in general) have improved in terms of capacity, efficiency and sophistication.

More than becoming part of almost every activity, the access to Information Technologies (ICTs), its use and interaction became synonymous with development (Lévy, 2003; Castells, 2005). In this sense, the politics of developing information technologies in order to decrease even more the prices has been implemented, while many initiatives of making the internet available to people in underdeveloped countries have been encouraged. For example, Information companies such as Google or Facebook have implemented measures to provide access to the internet to remote parts of Africa (Thielman, 2015). Non-profit organizations also joined this initiative. The World Telecommunication Union, for example, dedicated some meetings and conferences to overcome what is known by digital divide \(^{25}\) (ITU, 2016).

To sum up, the technological development, mainly in the Information Technologies represents a major sector of the contemporary globalized and interdependent economy (Albert & Papp, 1997). ITs and their growing availability create the advent of what Castells calls the ‘IT Paradigm’. Considering that 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).

The evolution of ITs has enabled an independent globalized public space not monitored by the state, nor manipulated by any other actor. This ‘space’ (in particular the Internet and its tools), can be defined as cyberspace. The latter has become a common mechanism for social interaction, allowing actors to meet and develop their interests in a very dynamic network. This was clearly defined by the Spanish National Cybersecurity Strategy \(^{26}\) (2013):

---

\(^{25}\) As defined by Internet World Stats, Digital Divide, digital split or digital gap refers to the amount of information between people who have access to Internet and those who lack it (Internet World Stats, 2016).

\(^{26}\) There is no consensus over the definition of cyberspace. Despite the similarities, the definitions of the concept of cyberspace may vary according to the methodological, theoretical or strategic goals of the actor who is defining it. For the purposes of this paper, we believe that the Spanish National Cybersecurity Strategy fits better in our discussion because not only does it involve technical elements, but also the interaction of social dynamics. For different definitions and a glossary, refer to [https://ccdcoe.org/cyber-definitions.html](https://ccdcoe.org/cyber-definitions.html)
Cyberspace, the name given to the global and dynamic domain composed of the infrastructures of information technology - including the Internet - networks and information and telecommunications systems, has blurred borders, involving their users in an unprecedented globalisation that provides new opportunities and entails new challenges, risks and threats.

Among the challenges imposed by the cyberspace as a new element of contemporary society, a special attention must be given to security issues: terrorism, hacking of data, access control, operation of infrastructure and cyber warfare (Lewis, 2002). States and international organizations adopted certain actions to deal with cyber security threats and to promote the governance of internet. One of the most remarkable initiatives in this sense was taken by the North Atlantic Treaty Organization (NATO), who fostered the publication of the Tallinn Manual.\footnote{In 2007 a series of cyberattacks were perpetrated against Estonia’s cyber infrastructure. It put down all the online services of the country. Considering Estonia is one of the most “cyberized” countries in the world and that an important part of the services is made online, it represented a grave issue for Estonians. More than that, the suspicion that 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 focused their study on this episode.}

This work will investigate how governance on internet is being promoted in the particular case of Brazil. This South American country has developed a Legal Framework, called the Civil Rights Framework for Internet (CRFI), 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 in what is known as a Multistakeholder way of governance. Moreover, Brazil started a campaign in international fora to foster the governance of internet in a multilateral agreement under the aegis of international organizations.

Although former President Dilma Rousseff had defined CRFI as the world’s most advanced law in defence of internet (Palácio do Planalto, 2014), it comes with some problems. Some issues concern the role of the state, since it is not specific enough, and its contradiction with some other legal documents, specially when it comes to security and defence issues.

This work intends to analyse the role of Brazilian initiatives in promoting the governance of the cyberspace under the light of securitisation theories. This paper argues that while Brazil descaricifics 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-securitisation of the cyberspace, by not clearly limiting state action on this field. To develop this argument, this text is divided into three parts. Considering that the main theoretical framework for this paper lies on the Securitisation theory, the first part
is dedicated to sum up this view. Since the establishments of the Legal Framework for the Internet in Brazil are understood here as an ongoing desecuritisation process, this part also addresses the general concepts linked with this aspect of the theory. Turning into a more specific approach, the following parts will explore the availability and use of the Internet in Brazil and its legal framework for civilian purposes.

Theoretical framework and literature review: securitisation and cyberspace

The issues concerning national security are generally at the core of the state purposes. Nevertheless, the decision regarding what is a priority among the security issues is still a complex process. The latter is subject to several elements, such as personal evaluations, personal vs group interests, the personal understanding of the decision makers, the discourse of different actors. The discourse is a fundamental piece of this whole as it is used to justify the measures to be taken, to establish what is really a security concern and to define who are the actors responsible for taking the adequate policy.

The systematization concerning this decision process is set by the Theory of Securitisation, originally thought under the Copenhagen School of Securitisation and complemented by other scholars. Having underscored the relevance of the cyberspace issues in the introduction, this part will focus on the Securitisation and Desecuritisation processes and on a brief literature review on security of the cyberspace.

As argued by the theorists of the Copenhagen School, to become a security priority an issue must first be securitised. That means in practice establishing an existential threat to a referent object (Buzan et al., 1998). There is a need to adopt special measures to protect a possible threatened element (Taurec, 2006). This securitisation move can be seen as the first step of the securitisation process.

The discourses or speeches are crucial within the securitisation process. It is through the discourses that a threat can be addressed and a functional actor persuaded to take the necessary measures to protect the referent object. According to Weaver, “a designation of the threat as existential justifies the use of extraordinary measures to handle it” (2012: 54). The referent object is something central to a securitisation 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.

To sum up, according to the Securitisation Theory, the security issues consist of a successful speech provided by a securitising actor. This actor, or group of actors, targets an audience (citizens, decision makers, representatives, who have the authority to adopt policies) in order to justify the use of special measures to protect or to make the existence of the referent
object secure. In this case, security becomes a social-constructed issue and not a pre-established 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 securitising actor uses a rhetoric of existential threat and thereby takes an issue out of what under those conditions is normal politics, we have a case of securitisation (Buzan et al. 1998: 24).

As argued by Weaver (2005), while the securitisation 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 et al. (1998), securitisation is something to be avoided, because it causes distortions on the normal conduct and management of the security issues. As such, Weaver (1995) proposes the opposite movement, where a desecuritisation process will be able to bring the security discussions and decisions to the normal rules. Notwithstanding, the desecuritisation process has to be more accurately analysed mainly because the “desecuritisation move” may not be as clear as the securitisation one. In fact, the desecuritisation cannot always be seen as the opposite pole of the securitisation.

According to Weaver (1995), the desecuritisation process must be the main goal within a securitised context. The actors shall pursue the demobilization of the special measures that characterise a securitised process, and bring back the securitised issue to be treated in the normal realm of politics. As Weaver underscores, it is necessary to transform “treats into challenges, and security into politics” (1995: 60).

Despite its importance, desecuritisation is under-theorized and little explored in the literature dedicated to the theories of securitisation. Nonetheless, some authors highlight various elements that can be summarized in three aspects. The first is to avoid the discourse that formalises a securitisation process (Biba, 2013). The desecuritisation does not necessarily depend on a securitised context and can be conscientiously applied as a policy of prevention, as well as in an ongoing securitisation process. The second strategy for desecuritisation involves the management of the securitised issues. This strategy must consider important aspects and be very clear in order to prevent a (re)securitisation process. Finally, the third strategy is the one that most closely matches the process opposite to securitisation. It is implemented through the opposite discourse of securitisation, which aims at bringing the securitisation issue to the normal
politics. As Roe (2004) suggests, this process can be viewed as a transformation movement. Sometimes there is room for a combination of strategies. It seems to be the case of Brazil, as it will be explored in the following pages.

The security of the cyberspace has been analysed through several theoretical lenses, 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 rising of cyberspace for International Relations and for the state, as in Choucri (2014). Also, the role of the state in dealing with this relatively new environment is explored by Nye (2011) and Naim (2014). Notwithstanding, Castells (2005), in a broad sociological approach, treats the cyberspace as a new age with implications for the social configurations in general.

The securitisation approach for cyberspace is also explored by the security studies, including the original creators of the theory. Buzan et al. (1998) mention the work of Nierop and Der Derian, to underscore that the rise of cyberspace may become a security issue, due the globalisation process. This concern is also addressed by Buzan and Hensen (2009) as a matter of international security, mainly after the 2001 attacks in the United States. According to the authors, the particularity of the securitisation of the cyberspace lies in its permeability to several sectors. As the theory suggests, there are five main sectors in security issues: Societal security, Economic security, Environmental security, Political security and the traditional Military security. The securitisation of cyberspace has implications in more than one sector at the same time. This issue was further explored by Hensen and Nissembaum (2009). The authors suggested that the securitisation of cyberspace occurs in three specific categories:

a) Hypersecuritisation: 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) Technification: limiting the security in the cyberspace to a high level of technical experts, bringing the decisions out of the political realm, as defended 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 securitisation of cyberspace (Ball, 2011). Some authors have already analysed this dimension. Caveltiy (2012) at some point understands that while cyberspace can be seen as an element of national security, it may be applied to military matters, since it can become a priority and a sensible point of reflection for national interests and protection. In fact, some countries have military divisions in charge of the protection of cyber activities, considered strategic for the governments.
The military dimension also meets the cyberspace specifically in this securitisation approach. As Hare (2010) elaborates, a military aspect conjugated with the social-cultural cohesion of a country can provide a set of elements to characterise and compare the securitisation 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 securitise cyberspace, contrary to stronger states. However, despite of presenting interesting elements to be tested as a theory, this model was not applied to any concrete situation.

There are few mentions to the desecuritisation of cyberspace, mainly because such approach needs to be developed both on its theoretical and empirical aspects. Giacomello (2007) suggests that countries such as France and the United States, persuaded by the private sector, are regularising the use of encryption instruments by civil consumers instead of keeping it restricted to the military sphere. An interpretation is possible here. As the desecuritisation passes through a process of regularisation by the state institutions, this can be seen as a type of ‘desecuritisation move’ that could bring back a securitised instrument (in this case, the encryption) to the normal ways of conduction of rules and uses.

In order to investigate the Brazilian initiatives concerning the cyberspace, it is useful to have a look at the Brazilian cyberspace situation. The next part will thus present a brief background on how representative and important the cyberspace is both for the Brazilian users in general and for the government.

The evolution and use of cyberspace in Brazil

Brazil has been witnessing a steady increase in the use of internet 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 centres. While the activities on the internet crossed the boundaries of academic and scientific fields to become a business issue, the infrastructure of connections and hardware were ameliorated. Besides, its prices decreased. As a result, the number of users increased, which made the government and companies 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 for generating more than 20 billion dollars (Statista, 2016). Furthermore, important activities like Internet Banking, social networks and e-governance services, are among the most developed and diffused activities in Brazil. It is indeed due to such activities that Brazil is considered the most ‘cyberized’ nation in Latin America, as well as one
of most cyber-inclusive nations in the world. However, there are here some big gaps 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 created institutions to address internet-related issues, from the regulation of the role of users and service providers, to more complex security matters involving military and strategic decisions at the state level. According to Diniz et al (2014), many of the entities are linked to the technical management of systems.

The implementation of policies, as well as the elaboration of legal and normative guidelines, are supervised by a few but very important institutions, which are in turn subject to a political hierarchy. The President of the Republic is the head of the organization that includes governmental institutions like the Brazilian Intelligence Agency (Abin), the Ministry of Defence, the National Defence Council, the Armed Forces and the Join Chief of Staff, and the Federal Policy.

Brazil has recently published its security strategy, which is split in two main documents: the National Strategy Defence (2008) and the White Paper to Guide Future Defence Priorities (2012). In what concerns cyberspace policies, the country published the Green Book on Brazil’s Cybersecurity in 2010 (Presidência da República, 2010). Among all, the most important document in this field is the CFI, which was approved in 2014 and regulated by former President Dilma Rousseff in 2016. The hierarchical relations among these institutions can be found in Diniz et al. (2014). The authors offer a visual scheme of the Brazilian main institutions and their relations with cyber security and the defence structure (figure 1).

The Security Discourse and the Brazilian Civil Framework for the Internet

Beyond the security concerns, cyberspace has become an object of domestic and foreign policy. The importance of cyberspace as a strategic security sector and its implications for foreign relations, was addressed by the former Brazilian Minister of defence in 2013, Celso Amorim. The discursive connection between security and cyberspace was unraveled when the 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 leaders and high authorities from several countries, sponsored by the American government (Greenwald, 2015).

In what concerns Brazil, the American agency 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 highlighted this event, as it became a very sensitive international issue.
As a result, this episode had many implications for the political field, at both domestic and international levels. In terms of foreign relations, Snowden’s revelations provoked a diplomatic dispute between Brazil and the United States and led Brazil to officially convey its discontent. The bilateral relations witnessed a huge setback, although not to the extent of cutting diplomatic ties. Rousseff cancelled a scheduled visit to Washington (Monteiro, 2013), and the Brazilian Ministry of Foreign Affairs, the Itamaraty, issued a note addressing some important elements. It classifies the act of espionage perpetrated by the American government as a serious attempt against national sovereignty and individual rights:

Illegal practices of interception of communications and data from citizens, companies and Brazilian government officials are a serious issue and a threat to national sovereignty and to individual rights, and incompatible with the democratic coexistence between friendly countries (Free translation from the original Palácio do Planalto, 2013).

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

Mr. President, we face a serious case of violation of human rights and civil liberties. The invasion and capture of sensitive information concerning business activities and, above all, a disrespect for the national sovereignty of my country. We made known our protest to the U.S. government, demanding explanations, apologies and assurances that such actions will not be repeated (Free translation from the original Palácio do Planalto, 2013).

The espionage scandal has pulled this discussion towards the approbation of what became known as the Civil Framework for the Internet28 (Palácio do Planalto, 2014b: online). Although it wasn’t directly associated with the Snowden case and was actually criticized by some civil sectors, the Civil Framework for the Internet was approved by the Brazilian congress in 2014. Although the law does not comprise any article that explicitly tackles the protection of the country against espionage, that issue itself was the object of debate by some parliamentarians. As this approach for security constituted some valorous argument for the approbation of the CFI which could be interpreted as a securitisation move, but not necessarily a complete securitisation process, the document itself does not extend to security issues, which can also be interpreted as a flaw in Brazil’s cyberspace and cybersecurity politics.

Despite the avoidance of the securitisation discourse, several actors choose to raise some security issues. They suggest the implementation of tools to avoid the securitisation in an attempt to establish or create ways to deal with similar situations. It is possible to link this movement to the aforementioned way of securitisation, namely, the management of the securitised issue. In this case, there is not a proper securitised topic. A contrary movement of securitisation can also be observed as the alleged intentions for the approval of the CFI were made towards a more democratic cyberspace. These intentions have the potential to bring some issues to a normal set of rules to be applied in their normal juridical aspects.

The approved set of rules was highly questioned. In fact, the final document lacked articles concerning some aspects of the cyberspace, including the role of the public power in security and defence. The next part will focus on the main aspects of the Legal Framework for the Internet.

28 It is important to emphasise that the CFI was proposed as a project of law by the Presidency of the Republic, in 2011, already under Rousseff’s mandate. This initiative precedes any denounces of espionage or security issues for cyberspace made 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, such as in Grossmann (2012).
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” (Brasil, 2014). The intentions (presented on Chapter one) include recognising the global scope of the use of internet and mentioning some important elements related to the protection of data and to the neutrality of the networks.

The document defines the elements of the internet upon which the law will be applied:

[The Internet is] the system consisting 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 from the original Palácio do Planalto, 2014b).

Additionally, the CFI is presented as a complementary law to the existent one and offers 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. As such, given its borderless features the extension of the internet, represents an ongoing debate, not only for Brazil but for the global governance of the internet.

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 governance and transparency, as well as the official information of private, public and academic sectors. The security issues are left for those who have the expertise, namely at the state level, the Cyber Command of the Army who shares this responsibility with the private sector. The role of both the state and the security agents in case of an alleged threat, such as espionage, theft of financial data or even theft of industrial information involves a military and strategic decision and not necessarily a public discussion.

Although claiming to be comprehensive, the Framework is 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 its utmost users in Brazil.

29 The final text of the law can be found at 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.
Conclusions

The structure of the CFI could be an interesting, yet imperfect tool to set principles for a secure legal framework for cybersecurity in Brazil. In other words, the document seems to be vague when it comes to security issues. Actually, it only acknowledges some generic security issues without mentioning the leading institutions and organs responsible for this subject.

The evocation of security aspects when the discussions for the approbation took place suggests the beginning of a securitization process. In fact, cyberspace was not fully securitised and the technical matters were delegated to a military branch that kept it as a high-institutionalized policy. By alluding to the public’s opinion, the press etc., the government managed to politicise this issue, amplified by Edward Snowden’s denounces.

Although portrayed by its proponents as one of the most advanced legal settings dealing with the rights and duties in cyberspace, the CFI didn’t prevent some controversial decisions such as the prohibition of WhatsApp for allegedly not cooperating with justice, and the imprisonment 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 the states’ duties, the CFI leaves some loopholes in the securitisation of cyberspace in Brazil, depending on the interests of the state or the government. Furthermore, issues dealing with cybersecurity in Brazil, as in many other countries, are mostly technical issues that fall under the military’s responsibility, which is aligned with the technification argument for the securitisation of cyberspace.

In a globalized world, cyberspace and cybersecurity are quintessential to our daily lives. In order to keep cyberspace de-securitised, not only does it have to be politicized, but also examined on two different levels. At the micro level, the technical aspects have to be probed in order to address the challenges. In turn, at the macro level, one has to study its implications on the society in general.
References


