Revista Jurídica vol. 02, nº. 55, Curitiba, 2019. pp. 592 - 606

DOI: 10.6084/m9.figshare.12041847

STRUCTURAL WAYS OF GOVERNING THE INTERNET –THE BRAZILIAN POSITION

MEIOS ESTRUTURAIS DE GOVERNANÇA DA INTERNET – A POSIÇÃO BRASILEIRA

PAULO GUSTAVO GONET BRANCO

Doutor em Direito (UnB), LL.M (University of Essex, UK), Professor do Mestrado/Doutorado do Instituto Brasiliense de Direito Público – IDP. Membro do MPF.

PEDRO HENRIQUE DE MOURA GONET BRANCO

Acadêmico de Direito (UnB). Visiting student da UC Berkeley.

ABSTRACT

The article addresses the peculiarities and complexities of the cyberspace regulation, acknowledging, but not endorsing, the utopic ideal of the cyberspace as a no-law virtual territory. It explores the variety of means of regulating people interconnections around the Globe through the Internet. It points up the need of due heteronomous protection of interests and claims linked to the core proposes of the Internet itself, such as those deriving from the freedom of expression and concerns with the right to privacy. The article takes as standing point Lawrence Lessig's pathetic dot theory about the four forces that design the use of Internet potentialities. It then focuses on the Brazilian current basic cyberspace normative framework and refers it to Lessig's theory, mentioning challenges yet to be met. It intends to share the Brazilian experience with the large English speaking auditory, pointing out how Brazilian legal framework relates to mainstream academic approach to Internet regulatory issues.

DOI: 10.6084/m9.figshare.12041847

KEYWORDS: Cyberspace Regulation; Internet; Pathetic Dot.

RESUMO

O artigo examina as peculiaridades e complexidades da regulação do cyberspace, aludindo ao ideal utópico desse espaço como um território virtual plenamente autônomo, mas não endossando essa postura. Explora a variedade dos meios de regulação das interconexões que a Internet propicia em todo o mundo. Assinala a necessidade de que interesses intimamente vinculados aos propósitos mesmos da Internet, como a liberdade de expressão e inquietações com direito a privacidade, sejam devidamente regulados de modo heterônomo. O artigo parte da teoria pathetic dot de Lawrence Lessig sobre as quatro forças que conformam o uso das potencialidades da Internet. Em seguida enfoca a estrutura normativa básica brasileira, referindo-a à teoria de Lessig e mencionando desafios ainda a serem enfrentados. O artigo intenta compartilhar a experiência brasileira com o mais largo auditório do público que se comunica em inglês, apontando como a estrutura normativa brasileira se relaciona com as mais modernas e importantes contribuições acadêmicas sobre regulação da Internet.

PALAVRAS-CHAVE: Regulação do Cyberspace; Internet; pathetic dot.

INTRODUCTION

The Internet blew out physical barriers between people living in the most different latitudes. The notion of time, associated to territorial distances, has received a substantial new meaning, under the possibility of the most intense and immediate interaction between people largely apart from each other. It is not improper to recognize that the Internet created a new kind of citizenship, composed of universally and highly interrelated *netcitzens.* There is a new parallel virtual society in which the development of our

DOI: 10.6084/m9.figshare.12041847

personality has the importance that the material growth we were used to had until recently. That brings new responsibilities and unimagined before trials to accommodate conflicting values and common concerns peculiar to this virtual society into civilized patterns.

Countries around the world are taking normative measures to meet those unavoidable challenges. This article intends to show how Brazilian legal framework is dealing with the most acute problems of the Internet and how it can be understood and valued under a mainstream academic approach to cyberspace regulatory issues.

2 NEW SOCIETY, NEW LAW

If it is true that the Internet has shaped a new society, it must also be true that a new Law framework ought to be established for this new society, making good the old Latin saying *ubi societas ibi jus* – where there is society, there is Law. The question is *quid juris* - which Law? The pursuit of an environment in which people interact with each other complying with certain guidelines that stabilize expectations sure enough is not to be shrugged off in the new society the Internet has carved. We are called to face a particular challenge on how to maintain an efficient and well structed social order in a world not of atoms, with specific boundaries, but of bits, where everything seems disperse[1].

Surely, alongside the shortened physical distances, the Internet brought about new ways of social interaction, changing the traditional notion of society. Manuel Castells (2005) was led to name this new form of sociability where people begin to interact in an environment without fixed boundaries – the cyberspace – as *Network Society*.

The amazingly immensity of this new virtual world is in itself a source of concerns. The breadth of a system that nevertheless allows the coexistence of micro-communities is a noteworthy difficulty in regulating this emerging society. Van Alstyne and Brynjolfsson (1996) called this phenomenon of some troublesome consequences *cyberbalkanization*.

[1] The distinction between a world of atoms and a world of bits was made by Murray (2016).

DOI: 10.6084/m9.figshare.12041847

The term *cyberbalkanization* itself reveals some of the startling issues one has to cope with when dealing with regulating Internet. The word embodies a paradox. It comes from the Turkish word *Balkan* which means mountains – physical barriers –, whereas the cyberspace destroyed physical hurdles. The oxymoron points out that in an environment where one may select his acquaintances by criteria other than geographic ones, people show tendency to interact only with like-minded individuals, weakening social ties with a macro-community. In addition to psychological problems that such posture may bring, it also makes harder to regulate the cyberspace and the Internet.

When one experiences no attachments to a larger social group – the macro-community –, it is unlikely that there will be enough common social values to create a body of law able to bind the whole cyberspace community. “Individuals [will] seek to obtain the best regulatory settlement for their community rather than for the macro-community at large” (MURRAY, 2011, p.4). It also makes barely impossible to regulate the Internet with traditional law enforcement means, which requires legitimacy to exist – since that legitimacy in a contractualist perspective comes from consent. As the common world clearly reveals, it is hard to foresee the possibility of creating laws able to convey a world-wide set of principles common to all citizens.

That does not mean, however, that the cyberspace is impervious to regulation, but that lawmakers will have to innovate and change concepts for the purpose of regulating. In this context, two opposite schools of thought emerged to deal with the best way to regulate the Internet, the so-called cyberlibertarianism and the cyberpaternalism.

3 CYVBERLIBERTARIANISM

The main theorist of the cyberlibertarianism doctrine is John Perry Barlow, who wrote in 1996 the Declaration of the Independence of Cyberspace. His theory was based on the lack of legitimacy of real-world government and laws to interfere in this sovereign space detached from the real space. He claimed that the cyberspace was a place where

DOI: 10.6084/m9.figshare.12041847

one would have to cross a virtual border to enter; therefore, the netizens were floating above the real world.

Barlow argued that only with the consent of the citizens of the cyberspace a regulatory system would thrive. He genuinely believed that one could go inside this new virtual world in the same way that someone takes an airplane to enter another country. This proposed new "country" would be a "world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity" (BALOW, 2001).

It is not hard to realize how utopic this perspective is. It is impossible to be transported to a physical cyberspace; Internet users are always under some jurisdiction. Moreover, law is necessary to give safety to social interactions and to allow businesses to flourish. From this perspective emerged the cyberpaternalism doctrine.

4 CYBERPARTERNALISM AND A NEW *LEX MERCATORIA*

The so-called cyberpaternalism asserts that the cyberspace is not resistant to real-world regulators. Joel Reidenberg was one of the first scholars to endorse this idea. He brought from the 11th century the idea of *Lex Mercatoria*, the body of law originated with merchants who needed to regulate their businesses regardless of their location. Once the law could vary in substantial matters between places where they use to trade, those merchants started solving their problems based on mercantile customs. It resulted in a codification able to provide certainty for their economic activity despite the jurisdiction under which they were submitted.

Reidenberg's idea was to apply the same principle adopted by the 11th century merchants to the Internet users. The purpose is to grant legal certainty to online citizens who may be under several jurisdictions at the same time – think of a Brazilian citizen living in The Netherlands accessing an American company website hosted in India by a British corporation. He supports the idea that a law made by the government is not the only

DOI: 10.6084/m9.figshare.12041847

source of rulemaking, but that "technological capabilities and system design choices impose rules on participants" (REIDENBERG, 1997, p.554). This set of rules forms what he named *Lex Informatica*.

5 THE PATHETIC DOT THEORY

The concept created by Reidenberg is intimately connected to the one presented by Lawrence Lessig, the 'Pathetic Dot Theory' (LESSIG, 2006). Lessig proposes that individuals are controlled by four forces that act together to regulate their lives. Those are Law, (Social) Norms, Market, and Architecture. Law refers to the traditional mechanism the government has to constraint someone, by the threat of punishment; (Social) Norms refer to the standards expected by the average of the citizens of a given society; Market refers to the influence that prices and other economic issues have on someone's behavior; and Architecture refers to the design of a system – limits imposed by the way that something is created.

Lessig's point is that those constraints regulate both real-world and virtual interactions. The sale of alcoholic beverage is an example of a real-world activity regulated by the four modalities. In Brazil, the law determines that one has to be over eighteen years old to buy alcohol. This legal requirement is a constraint on individuals under eighteen who intend to drink. Social norms also act as a constraint to the relation between individuals and liquor. Social norms say that one should not drink early in the morning nor excessively. Those who break such social expectations will suffer sanctions, from criticism to ostracism. Market too interfere in the use of alcohol, for example by setting prices that control the amount of drinks one can have. Finally, the architecture of alcoholic beverage inhibits people from drinking unrestrainedly. After certain amount of ingested alcohol, the body reacts in a way that make it uncomfortable for individuals to keep drinking.

The regulation of drinking, therefore, is determined by those four limiting aspects of life – laws, norms, market, and architecture. They interact with one another and the

DOI: 10.6084/m9.figshare.12041847

sum of their activity regulates everything. Each of the four elements prevailed in specific periods of the past three centuries. Lessig suggests that in the 19th century the main constraint of social life were social norms; in the beginning of the 20th century, laws were preeminent in guiding one's action; in the middle twentieth, market was the great regulator; and the 21st century is experiencing the prevalence of the architecture as the most important behavior controller.

Lessig argues that these four patterns of regulation are observed in the cyberspace. He stresses that, given the peculiarities of the virtual world, laws there are not the most important constraining element. The architecture of the Internet is the main phenomenon that sets limits to activities and choices.

Explaining the architecture element, he points out that just like bricks and cement shape a building – functioning as its architecture –, a set of code, composed by hardware and software, is the constituting part of cyberspace – the platform. "The software and hardware that make cyberspace what it is constitute a set of constraints on how you can behave. […] They constrain some behavior by making other behavior possible or impossible" (LESSIG, 2006, p. 124).

He proceeds mentioning that the code "embeds certain principles; it sets the terms on which one uses the space; it defines what is possible in the space. And these terms and possibilities affect innovation in the space. Some architectures invite innovation; others chill it" (Lecture given at the pcForum in 2000, USA) That is why Lessig advocates that the code is the most important constraint when it comes to the regulation of the Internet.

He argues that "one obeys these laws as code not because one should; one obeys these laws as code because one can do nothing else. There is no choice about whether to yield to the demand for a password; one complies if one wants to enter the system" (LESSIG, 1996, p. 1408). From this assumption comes Lessig's famous quote that code is law, meaning that code is the main entity controlling behavior online.

This reality yields an important consequence. Government and market actions aiming to regulate the cyberspace and to promote fundamental values depend on

DOI: 10.6084/m9.figshare.12041847

influencing the architecture of the virtual world – the code. Music streaming services provides an example of it. Aiming to fight piracy, companies like Spotify proposed a model that would make it easier and simpler to buy music that to pirate it. Paying a specific amount every month would give easy access to great part of the most known songs ever created. Before Spotify, "the clash between online behavior and compliance with legal regulation was conflated with the mismatch between socio-technological change and the legal path" (SUN, 2018, p. 142). The market was able to create a system that made it easier to respect property rights than to commit piracy. The code was built in order drive people to comply with the law.

Governments too should create laws to influence the structure of the Internet. The United Kingdom government, for example, requires Internet Service Providers (ISP) to "place technical measures to prevent their customer accessing websites containing illegal images of child abuse" (MURRAY, 2013, p. 77). The identification of such websites is made in partnership with the Internet Watch Foundation (IWF). This is an instance of a state law aiming at the architecture of the Internet. If ISP blocks access to a website, the final customer will not be able to view the illegal content. That is why Lessig says that obeying the law as a code is not *an* option, but the only one.

6 THE BRAZILIAN LAW'S APPROACH

As it has been shown, "in the man-made environment of the digital sphere, our ability to change the design of that place with a few well-placed keystrokes means that the use of architecture as a modality of control is increasingly in evidence and is increasingly effective" (MURRAY, 2013, p. 76). In this perspective, "government should take steps that induce the development of an architecture that makes behavior more regulable" (LESSIG, 2006, p.62).

Pursuing that objective, Brazil was in the vanguard of the regulation of the Internet when it created what The Economist coined as the "Magna Carta from the Web" (THE

DOI: 10.6084/m9.figshare.12041847

ECONOMIST, 2014). The bill passed in a peculiar context. It came to the attention of Brazilian authorities and public opinion the Edward Snowden allegation that NSA's surveillance program was monitoring Brazil's telecommunication system and that political and economic sensitive information were being gathered. This was a strong push to Brazil enact the 2014 *Marco Civil da Internet (MCI)* – the Brazilian Civil Rights Framework for the Internet.

The framework is relevant because it was originated from a multistakeholder process, which brought together civil society, especially private sector entrepreneurs, and State to draft the Internet Bill; and because it joints in a single document the main legal provisions related to the cyberspace. As stated by Tim Berners-Lee, the inventor of the World Wide Web, the Brazilian *MCI* "protects and expands the rights of users to an open, free, and universal web" (Speech given at NETmundial conference in 2014, Brazil).

Another regulatory framework that will shape the Internet in Brazil is the General Data Protection Law – *Lei Geral de Proteção de Dados (LGPD)*. It deals specifically with data protection, whereas the *Marco Civil da Internet* regulates the relationship between Internet Service Providers and users. Those statutes constitute the major legal constraints of the Internet in Brazil.

7 BRAZIL'S CIVIL RIGHTS FRAMEWORK FOR THE INTERNET – *MARCO CIVIL DA INTERNET - MCI*

The *MCI* is the legal framework that addresses freedom of speech per se. It deals with the issue of filtering, which has, in Lessig's words, "undeniable value […]. We all filter out much more than we process" (LESSIG, 2006, p. 259). Using filters is intimately connected to the role played by private regulators in cyberspace. Once ISPs control who have access to the Internet – an architecture issue –, they fulfill an essential role in safeguarding illegal forms of speech, such as spam, child porn, and hate speech. The *MCI* imposes some obligations to service providers, like blocking websites with such

DOI: 10.6084/m9.figshare.12041847

content. Even though the simple fact of filtering may leave loopholes for malicious people, one may well endorse Lessig's reasoning that "regulation does not need to be perfect to be effective. It is enough that these regulations make porn [or other illegal material] generally unavailable" (LESSIG, 2006, p. 247).

The problem here is that some judicial decisions were adversely affecting tech companies like Facebook and Google, making it unattractive for market firms to keep operating in Brazil and arising issues of danger to democratic speech. For example, a Brazilian intermediate court found Facebook liable for material made available by a student who was criticizing a city councilman. The politician had required the exclusion of the post, but Facebook only did it after judicial order. Nonetheless, the Internet company was condemned to pay the equivalent of nine times the minimum wage for the representative. It is arguable that the obligation of removing every single post that users dislike could make Facebook's activities inviable and freedom of speech would suffer an enormous injury.

The law made an option to make ISPs liable for the content they make available only if a judicial order determines the removal of the post (*MCI*, article 19). One need to submit an application before a court in order to prove a violation of one's right and then get a judicial order to block such content. It means that people can make their points and support their ideas regardless of state interference, unless it fits the specific group of unlawful speech – for both *real* and *virtual* environments. The *MCI* opts to only make it a duty to ISPs to remove a content if a judge orders it, establishing a system of balance between personal rights and freedom of speech that clearly favors, prima facie, the latter.

Anyhow, at this point the law gives a clear example of a statute that influences the code and helps the state to achieve a good regulatory level – once material is proven inadmissible it becomes not available and people are simply cannot access it. That's how government may control what John Perry Barlow argued to be uncontrollable.

Sure, one still depends on the sensitivity of judges to deal with cases that may not be easily approached. One cannot even dismiss the risk of judges influencing the code clumsily, producing unappropriated judicial orders. In 2016, a criminal judge of a small city

DOI: 10.6084/m9.figshare.12041847

(100,000 inhabitants) ordered Brazilian ISP's to block the text messaging app WhatsApp access for everyone in the Brazilian territory. The request came after Facebook – that owns WhatsApp – refused to obey a previous order in a criminal investigation requesting a breach of confidentiality in a suspect's phone. The judge decided based on the article 12 of the *Marco Civil da Internet* which allows the temporary suspension of activities that entail events set forth in the law.

This was a manifest case of law misunderstanding, affecting the code in an improper way. But it was not the only extreme case of misapplication of the Internet Law. Also in 2016, the same judge who ordered the block of WhatsApp determined the imprisonment of Facebook's Vice-President for Latin America for not giving access to private messages exchanged in WhatsApp. These controversial decisions prove that the law is efficient to regulate the cyberspace, but that one must care for its enforcement in order to prevent drastic and disproportionate situations like these. Cyberspace has to be regulated respecting democratic guidelines and also law enforcement has to be oriented by the same principles.

8 INTERNET, PRIVACY AND DATA PROTECTION IN BRAZILIAN RECENT LAW

The legal framework that addresses right to privacy per se is the *Lei Geral de Proteção de Dados*. Following the example of the European General Data Protection Rights (GDPR), the Brazilian parliament approved in 2018 the new data protection law which will come into effect in 2020 (Law #13.709/2018).

The first article explains the LGPD's goal: to regulate the way natural person and legal entities – of private or public law – process one's personal data. The definition given for personal data is very broad: "information regarding an identified or identifiable natural person" (LGPD, Article 5, I). It means that even when the data does not clearly identify someone, the law protection applies inasmuch as someone's identity may be inferred. It becomes especially relevant when one deals with Big Data – extremally large data sets –

DOI: 10.6084/m9.figshare.12041847

that will be under the law regulation, whenever containing information considered personal. However, since the available technical means is insufficient to identify a subject, the data collected will not be protected.

Grounded on the respect for privacy but also on freedom of expression – as stated in Article 2 – the law excepts from its range of protection the processing of data done exclusively for journalistic, artistic, and academic purpose; as well as when it is made in name of public safety and national defense. The protection is more sophisticated, though, when the data is considered sensitive, defined in Article 5 as "personal data concerning racial or ethnic origin, religious belief, political opinion, trade union or religious, philosophical or political organization membership, data concerning health or sex life, genetic or biometric data, when related to a natural person". Sensitive data are covered by some additional security layers, such as the express consent of the data subject, are required.

Another important element of the law determines that "processing agents shall adopt security, technical and administrative measures necessary to protect personal data from unauthorized accesses and accidental or unlawful situations of destruction, loss, alteration, communication or any type of improper or unlawful processing" (LGPD, Article 46). Article 42 establishes that the controller and/or the processor that miscarries their activity and causes "material, moral, individual or collective damage to others […] are obligated to redress it". The penalty for infractions my reach a maximum of fifty million reais [2].

The *LGPD* relates to all the four constraints proposed by Lessig. When it imposes a penalty for those who break the law, it stimulates the market to adapt and regulate its businesses to comply with what is determined. When it requires additional security layers for processing data, it forces a change in the code to fulfill the legal requirements. Finally, when it brings in its Article 2nd seven grounds of the regulation on personal data protection – principles that must guide the application of the law –, it dialogues with social norms, since principles depend on values that the society believes to be central to their lives.

[2] In 2019, approximately 13 million dollars.

DOI: 10.6084/m9.figshare.12041847

CONCLUSION

It is universally accepted that the Internet has turned old habits upside down, making common life exceedingly easier and less cumbersome. The Internet has fostered an unprecedent connection of people all around the world, promoting shared human rights values. Information is gathered and shared everywhere on the Internet and it has given commerce a new and an always expanding meaning. The web space knows no physical boundaries, nor its scope of action is restricted to any single country.

Such a revolutionary mark in human history could not fail to bring about new and hard challenges to social design. Just like merchants, in other era, created the *Lex Mercatoria* – a needed body of law that would give their business legal certainty –, online citizens and companies also look for safeguards to run their errands.

A sort of universal *Lex Mercatoria* is yet to be drawn, but it is possible to infer from current experience a set of necessary measures that each country is advised to build up in order to make Internet safer and to bolster the use of its social interaction potentialities.

Legal framework is to be carefully setup, and it must take into account the four elements that are crucial for the approach – Law statute itself, already developed Social Norms, Market and Architecture. It is also very much useful that international community be informed of how domestic legislation deals with these new challenges. This article hopes to give initial information on that regard about Brazilian actual stand.

Brazilian law is conceived upon the acknowledgement of the importance of the Internet to freedom of speech and other fundamental rights shared by international community. It also follows the idea of the European GDPR and foresees extraterritorial jurisdiction for data collected in Brazil. Its protection is not limited to citizenship, nationality of the personal data, neither to the residency of the titular of the data (PECK, 2018, p.29).

Brazil's legislation follows the ground established by the European Data Protection law and other governmental regulations of the Internet. It is able to deal with the main issues concerning online free speech and right to privacy.

DOI: 10.6084/m9.figshare.12041847

We can identify Lessig's proposal in the Brazilian regulatory system, where laws, market, and social norms act to shape the code – architecture –, in other words, those elements are taken into consideration to efficiently give shape to a desirable online behavior.

Like any other country, Brazil depends on the good will of its judges to properly address more complex cases, but the law is well delineated. It does not mean that there is nothing else to be done; on the contrary, as new technologies dawn, new legal rules must be created to protect the citizens from daily dangers. The advent of new technologies should also stimulate the government to be one pace ahead and shape the architecture of it, always aiming to protect freedom of speech, right to privacy, freedom of creation and of economic initiative, and all other principles essential for a safe and fulfilling social interaction.

REFERENCES

BARLOW, John. A Declaration of the Independence of the Cyberspace. In: LUDLOW, Peter. **Crypto Anarchy, Cyberstates, and Pirate Utopias.** Cambridge: MIT Press, 2001.

CASTELLS, Manuel; CARDOSO, Gustavo (org.). **The Network Society:** From Knowledge to Policy. Washington, DC: Johns Hopkins Center for Transatlantic Relations, 2005

LESSIG, Lawrence. **Code 2.0:** Code and Other Laws of Cyberspace. New York: Basic Books, 2006.

LESSIG, Lawrence. **The Zones of Cyberspace.** Stanford Law Review 48, no. 5, 1996.

MURRAY, Andrew. **Information technology law:** the law and society. Orxford: Oxford University Press, 2013.

MURRAY, Andrew. Internet regulation. In: Levi-Faur, David (org.). **Handbook on the Politics of Regulation.** Cheltenham: Edward Elgar Publishing, 2011.

PECK, Patricia. ***Proteção De Dados Pessoais*** *- Comentários À Lei n. 13.709/2018 (LGDP).* São Paulo: Saraiva, 2018.

DOI: 10.6084/m9.figshare.12041847

REIDENBERG, Joel. **Lex informatica:** The formulation of information policy rules through technology. Tex. L. Rev., 76, 1997.

SILVESTRE, Gilberto Fachetti; et.al. The procedural protection of data de-indexing in internet search engines: the effectiveness in brazil of the so-called “right to be forgotten” against media companies. In: **Revista Jurídica – UNICURITIBA,** v.1, n.59 (2019). Disponível em: http://revista.unicuritiba.edu.br/index.php/RevJur/article/view/3299/371371792.

SUN, Hyojung. **Digital Revolution Tamed:** The Case of the Recording Industry. Basingstoke: Palgrave Macmillan, 2018.

THE ECONOMIST. **The net closes.** (2014, March 29).

VAN ALSTYNE, Marshall; BRYNJOLFSSON, Erik. **Electronic Communities:** Global Villages or Cyberbalkanization?. ICIS 1996 Proceedings. 5, 1996.