SCIENTIARUM HISTORIA XII

Data protection and digital humanities in Brazil: black boxes

Proteção de dados e humanidades digitais no Brasil: caixas-pretas

Luiz Paulo Carvalho, Jonice Oliveira

Graduate Programme in Informatics (PPGI) – Federal University of Rio de Janeiro (UFRJ)

luiz.paulo.carvalho@ppgi.ufrj.br, jonice@dcc.ufrj.br

Received: 4/12/2019 Accepted: 8/12/2019 Published: 10/12/19

Abstract. *The effervescence of the theme of privacy and data protection around the world is growing, ranging from the preservation of the right to personality to the preservation of democratic principles as we traditionally know. Works have been developed seeking compliance with laws and regulations related to this theme, not observing a socio-technical epistemological side of digital humanities. In this paper I expose black boxes that communications make clear, serving as guide for further interdisciplinary research.*

Keywords: *General personal data protection law. Post-colonialism. Sociotechnical.*

Resumo. *É crescente a efervescência do tema de privacidade e proteção de dados pelo mundo, contemplando desde a preservação do direito à personalidade até a preservação dos princípios democráticos como tradicionalmente conhecemos. Trabalhos vem sendo desenvolvidos buscando conformidade com as legislações e normativas relacionadas com este tema, não observando um lado epistemológico socio técnico de humanidades digitais. Neste trabalho exponho caixas-pretas que as comunicações deixam perceber, e que podem servir como norte para pesquisas interdisciplinares posteriores.*

Palavras-chave: *Lei geral de proteção de dados pessoais. Pós-colonialismo. Sociotécnica.*

1. Introduction

On August 14, 2020, the Brazilian General Data Protection Act (*Lei Geral de Proteção de Dados Pessoais* – LGPD) will take effect [1], regulating the data protection operationalized by the handling of Brazilian natural persons data, in digital or physical scope, either internally, at national borders, or externally, in transnational scope.

[1] http://bit.ly/2PeKgcj. Access in 01/12/2019

In this paper I try to tension some opaque points about LGPD, outlining a research agenda with a socio-technical bias from the perspective of Digital Humanities. Given the focus of this work I will not go into detail in LGPD or European Union (EU) data protection legislation, the General Data Protection Regulation (GDPR) [2].

These tensions arise from “loose threads” in the maze of the political epistemologies of technologies, which lead to black boxes from the perspective of forming a semiotic-materialist network. I then use the Actor-Network Theory (ANT) approach (LATOUR, 2005) (LATOUR, 1987), where I analyze non-human as well as human actors as actors and participants in legal and judicial systems related with data protection in Brazil. In this research I am interested in black boxes, according to the ANT are actors or associations of actors, even whole networks, opaque and unidentifiable, purposely or not.

The roots of LGPD's final approval are associated with international cases of unscrupulous digital manipulation of personal data, such as Brexit and the 2016 US presidential election; as well as Brazilian cases, such as the 2018 presidential elections (BIONI, 2019). In certain cases, there is not even the need for sharing misinformation, commonly widespread as fake news, an informational biased approach associated with the target’s profile of interest may be enough to lead it to the expected behavior, even if that behavior is inaction. [3]. For example, encouraging the voter to be absent from an electoral process.

LGPD is generic to the point of abstracting media and channels, influencing both digital platforms and paper-based customer registration forms for small businesses. Considering processing capabilities, the emphasis is on the computerized category, operating on dozens of dimensions simultaneously, and not on the human category, which presents algebraic and graphical representation difficulties in surpassing three dimensions (SUMPTER, 2018). The importance of the media type will be deepened later.

As I have observed some communications using misleading or dubious terms, I characterize as necessary a clarification on Privacy and Data Protection differences. Through the communications can be found lines that mix the two terms or cite the LGPD as "privacy law", which is a semantic infidelity. Duties and legal obligations are related to positive law; The non-interference of some in relation to the rights of others is related to the negative right. As Bioni (2019) clarifies, Privacy has a negative aspect, it comes to light only when it perceives itself violated; Data Protection has a positive aspect, it is the duty and obligation of the State and Society to protect and preserve it. One way to preserve privacy is with data protection, but data protection does not come from privacy. From the moment someone decides to share your data, either by filling out a personal record, privacy is violated, even if sharing is only between that person and the organization that has provided you with certain security or data protection. For example, GDPR uses the principle of “Data Protection by Design” and not “Privacy by Design”, there is no quote from the latter in GDPR's core text, even if some communications, written or oral, make a mistake to cite differently. [4].

[2] http://bit.ly/35OtKWW. Access in 01/12/2019

[3] http://bit.ly/2ODFpCc. Access in 01/12/2019

[4] https://glo.bo/2sAncgl. Access in 01/12/2019

Considering the direction of the research, I structure the work as follows: Section 2 presents a brief history of data protection in the EU and Latin America; Section 3 presents the main tension of this work, the deepening of the Digital Humanities bias of the Brazilian data protection scenario, such as postcolonial bias, negative influences on the effectiveness of legislation, pancapitalist opportunism on legislators, among others; Section 4 presents the conclusion.

2. Brief Data Protection History

In Brazil, some points prior to LGPD are considered precursors of data protection, among them Articles 43 and 44 of the Consumer Protection Code (Código de Defesa do Consumidor – CDC) [5], from 1990; Brazilian Civil Rights Framework for the Internet (Marco Civil da Internet – MCI) [6], from 2014. On the latter is Article 7, which was supplemented before final approval by receiving specific items for personal data protection over the Internet. The "data protection injection" at MCI was influenced, as a Brazilian response, by Snowden's revelations about US government's unethical and illegal espionage initiatives (BIONI, 2015), not just about citizens of other countries, but also of heads of state, the government. Paragraphs I and II of the MCI show explicit concern for communications confidentiality and their respective flows.

The first proper data protection law in Brazil is the LGPD. Its beginning dates to 2010, where the debate on the theme was opened for the whole society. After a latency period is resumed in 2015, where a new collaboration platform was used (BIONI, 2015). The term "general" in LGPD comes not only from the multisectoral breadth that the legislation spans, but also from the rich multisectoral collaboration that culminated in the final drafting of the legislation, with broad and democratic participation by a portion of interested and engaged society, not just legislators and lawyers (BIONI, 2019).

Countries very close from Brazil, geographically and geopolitically, already had its own and dedicated data protection laws, for example: Argentina, 2001; Chile, 2002; Uruguay, 2008; and Colombia, 2012 (DLA PIPER, 2019). These countries also have operational and controlling entities of their respective laws, different from Brazil. In Brazil, the entity responsible for data protection, in the light of LGPD, is the National Data Protection Authority (Autoridade Nacional de Proteção de Dados – ANPD), already effective by LGPD itself, but not composed and in fact established, its members have not yet been all defined, so far.

The Southern Common Market (Mercado Comum do Sul – Mercosul) was founded in 1991, the last country to access the group was Venezuela in 2012; This same country has been in suspension since 2016. Mercosul is made up of five full members: Argentina, Brazil, Uruguay, Paraguay and Venezuela; five associated countries: Chile, Bolivia, Colombia, Ecuador and Peru. By simple association, Mercosul would be the equivalent of the European Union of South America.

[5] http://bit.ly/2RcOQKv. Access in 01/12/2019
[6] http://bit.ly/2CBJrVk. Access in 01/12/2019

In Europe, the history of data protection is more distant. Date 1981 with the Data Protection Convention (DPC); in 1995 with the European Data Protection Directive (EDPD). In 2012 GDPR comes to light and is put into multisectoral debate by European society, being approved 4 years later, in 2016, and coming into effect in 2018. GDPR covers all EU member countries. Several treaties formed the EU as it stands today, from the Treaty of Rome in 1957 to the Treaty of Lisbon in 2007. In 2013 Croatia became the last country to join the EU, being the 28th.

3. Digital Humanities and Data Protection in Brazil

GDPR allows only countries with legislations that provide comparable data protection rigor to treat personal data or sensitive data of EU citizens. In this context we will return to the physical and digital media, if an EU citizen intends to host in Brazil, even if the specific business uses a physical all-paper register, he still needs to be GDPR compliant. The Brussels Effect (BRADFORD, 2012) helps us to understand the postcolonial phenomenon of legal colonizing influence in peripheral or semi-peripheral countries, through geopolitical vision, in countries that are dependent on negotiation with the EU. That is, the EU exports not only its data protection legislation, but also its principles, values and conceptual epistemologies on the topic (SCOTT AND CERULUS, 2018). How we understand and operate data protection is how the EU understands and operationalizes data protection.

Legal mechanisms and operationalizations, legal artifacts, are imported from another context, where the challenges and problems of Brazilian data protection are not necessarily considered. I note that communicators on the topic not only address GDPR for any neglected or missing topic in LGPD, but also recommend it to others: “If we cannot resolve this item in light of LGPD, we turn to GDPR, impacts and applications, to look for bases and examples of how to act here. ” Not only do we import the legal artifact in its essence, but we also import complementary information in advance, we decide specific national issues in the eyes of a very different sociocultural community. European contextual aspects are different or incompatible with Brazilians, such as economic, socio-cultural or the level of digital technological maturity (MOOR, 2005).

Following this context, Couldry and Mejias (2019) tackle postcolonialism and decolonization by dealing with data and its influences, citing Brazil and its relationship with GDPR. The first black box relates to the choice of the proposed EU data protection legislation. Whereas: (i) other countries much closer, geographically or geographically located in the global south, peripheral or semi-peripheral, already had well-established data protection laws, with their particular regulators and many years of practical effectiveness; (ii) the EU built its legislation as a unified group, leaving it open for each country to complement GDPR with its contextual additives; (iii) GDPR, since its approval in 2016, already recognized Uruguay and Argentina as countries with data protection initiatives in accordance with its rigor; (iv) the concern with data protection, physical or digital, dates back decades, intensified in the 1970s and 1980s in Europe and the United States, and was first outlined in the Brazilian CDC in 1993; I note: (a) Mercosur has not built its own consolidated data protection legislation, even if anthropophagized (MEDINA et al., 2014), based on the laws already in force in its member countries; (b) Brazil has not resorted to the laws of Argentina or Uruguay to build or base most of its own. It seems that GDPR, and its transnational data transaction restriction item, that really motivated this topic, not the provisions of Article 1 of the LGPD; (c) being primarily a pancapitalist precaution (ESCOBAR, 2018) to European sanctions and possible fines, then there is no material concern about privacy, freedom, data protection or the concept of good faith whatsoever. Following the reasoning of item (c) we can go downstream (LATOUR, 2016) of this network still in formation predating that LGPD may, in fact, act on markets and businesses superficially, neglecting other harmful side effects to the democratic social fabric, such as manipulation of data beneath the scenes to influence election results from operations that use personal data as profiling as input (PINTO, 2018). That is, the law will only serve “just for show to Europeans”, building a facade of "yes, as a country we are in compliance".

Another point beyond the Brussels Effect (BRADFORD, 2012) can be seen in a technical-linguistic colonization. In LGPD, roles with specific responsibilities are considered, the two with the greatest involvement in data processing being the *encarregado* (operator) and the *controlador* (controller). It reads: “controller: natural or legal person, whether public or private, who is responsible for decisions regarding the processing of personal data;” and “operator: natural or legal person, whether public or private, who performs the processing. personal data on behalf of the controller;”. GDPR considers the role of the Data Protection Officer (DPO), by simple analogy would be the equivalent of the controller in LGPD. Since the LGPD sanction, several actors, especially lawyers, have called themselves DPOs, although this role has no association with LGPD and is only in effect at GDPR. A quick search for the term Data Protection Officer on Google exposes the predatory and seductive environment for opportunists who perceive the European role as socially better capitalized than the Brazilian controller, even if it is ineffective indeed (CARVALHO et al., 2019).

With a technological bias (MARQUES, 2016), a major importation of GDPR to LGPD presents us with another black box: the technological equipment that will operationalize LGPD concepts. Considering that the dominant discourse of practice is to refer to GDPR, we can move in this thought to the respective existing technological devices. Who owns these GDPR compliant devices? The EU, whether specialized human resources apparatuses, potential consultancies; or the computerized technological devices such as Database Management Systems (DBMS) configured to the technical requirements from the LGPD or GDPR.

As a controversial topic regarding data protection, face recognition can serve as examples for another black box of the monopoly of personal data processing technology by private organizations. For example, public organizations do not own facial recognition algorithms. In the United States, several of the largest technology companies, such as Amazon and Microsoft, with facial recognition solutions, are pushing the government to create laws that regulate their use [7]. These companies not only call for regulations on the subject but draft their own laws and conceptualizations for these same regulations [8], explicitly demonstrating their intention to dominate the legal discourse on the subject. The reasoning is simply deduced: (1) face recognition technologies are being banned or

[7] https://engt.co/33Fu8Wm. Access in 01/12/2019
[8] http://bit.ly/2DCgqZA. Access in 01/12/2019

perceived infamously by the Society; [9]; (ii) major technology companies suspend the launching or spreading of their face recognition technologies, claiming that the providers of the services and their users are wrong; (3) the same companies put pressure on society, especially legislative actors, to think of "legal restraints" that "control" the use of the technologies they develop and make available; (4) legislators, lobbyists or not, call for specialized and empirical technological assistance on the subject; (5) Who holds the specialized and empirical know-how about facial recognition technology? The same companies that develop and make them available; (6) next step for these companies? Draft their own regulations on the subject, as if acting in good faith. Zuboff (2019) will classify this "good faith" as inconceivable by the precepts of vigilant capitalism.

This illustration of the course of what has happened to face recognition in the United States may be associated with the GDPR and LGPD, as well as any future face recognition regulations that the global north will adopt. Thus, for example, a prelude to GDPR may, in the future, be that Amazon restricts the commercialization of its facial recognition technology apparatus only to countries that present legislation comparable to those it considers ideal, and this phenomenon may become a widespread behavior to other companies in the industry.

One of the cases of data protection, facial recognition, and tension of consent is the implementation of cameras of this technology in churches [10], or environments where there is an implicit power relationship, a hidden doctrinal curriculum. How can any legislation or public power compete against an alleged "sacred determination" through a possible "divine word" that orders members of that community to give consent to the handling of their image to the religious institution? In another scenario, how will an underprivileged employee report the misuse of its personal data or sensitive data at the institution in which work? How is an applicant for a job going to file a complaint because the selection process has attempted to collect data that is inconsistent with the purpose of the job for which access is sought? One challenge is to build mechanisms and operations that curb these false legitimate interests or unscrupulous predatory consent by empowering the data subject without exposing them to harm. Preservation of this data subject is also the prerogative of LGPD.

Finally, I make one last tension parallel to the sociotechnical view (CUKIERMAN, 2007) in relation to the Chinese Credit Score, together with the Social Credit System (SOARES, 2018). In China personal data and sensitive data are collected by super platforms such as Alibaba company. As in Brazil, technological data surveillance devices are owned by private organizations, which provide data to the state, due to the country's model. The state can then build scores and quantify citizens according to their data and their specific actions. The intention of the LGPD is mainly to prevent this phenomenon of total vigilance over people's lives. Nevertheless, the government seems to be going the wrong way, trying to build the National Register of Social Information (Cadastro Nacional de Informação Social – CNIS), through the decrees 10.046 and 10.047/2019. This unique database registration conflicts profoundly with LGPD's purpose of ensuring the widest possible right to privacy through the data protection consented by the natural person.

[9] https://nyti.ms/35QujPX. Access in 01/12/2019
[10] http://bit.ly/2P0tGfW. Access in 01/12/2019

These two decrees seek to collect personal data and sensitive data from the entire Brazilian population, with no purpose or other specific information available, with the justification of "fostering interoperability", "sharing databases" and "expanding information". That said, the state will have all the information possible and imaginable to build a total surveillance solution, containing from the address to a person's retinal data. The state itself, through a supposed power of action, completely violates the privacy of all Brazilian citizens in just two consecutive decrees.

4. Conclusion

LGPD finally brings the theme of Privacy and Data Protection "to the table" of the Brazilian. With the law less than a year to go into effect, spirits are high, and the outline of speeches is taking shape, explicitly or implicitly, for or against the law. As communications where authors uncritically prioritize elements such as “competitiveness”, “innovation” and “technological progress” [11], inserting several adverse conjunctions after stating the advantages and benefits of data protection in Brazil. Careful inspection is required in communications that try to appear neutral and impersonal or personal, and in their speeches. One approach is to use comic-like speech bubbles to track actors and their networks (LATOUR, 2016).

Already positioning myself fully in favor of the intention of the law, I also consider that we cannot renounce a deepening in the black boxes that make up the socio-technical aspect of this scenario, its actors and their respective networks. It is undeniable that there is a colonization factor in the act of importing most of the legal artifact (ESCOBAR, 2018), because not only by importing the law, we are importing the norms, customs and perceptions of reality from another context. And, concomitantly, we need to be aware of unscrupulous surveillance initiatives by the same state that has passed and will enforce data protection legislation that supposedly preserves the right to privacy.

Funding

This work was carried out with the support of the Coordination for the Improvement of Higher Education Personnel - Brazil (CAPES) - Financing Code 001.

References

BIONI, B. **Proteção de Dados Pessoais - A Função e os Limites do Consentimento**. ed. 2. São Paulo: Forense, 2019.

________. **Xeque-Mate: O tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. São Paulo: GPoPAI/USP, 2015.

BRADFORD, A. **The Brussels Effect**. Northwestern University Law Review. 107 (1). SSRN 2770634, Columbia Law and Economics Working Paper n. 533, 2012.

CARVALHO, L.P.; CAPPELLI, C.; OLIVEIRA, J. **Proteção de Dados no Brasil, uma visão Sociotécnica em Sistemas de Informação**. 2º Encontro do INCT.DD. Salvador, Bahia. DOI 10.13140/RG.2.2.13999.89765. 2019.

[11] http://bit.ly/33HR2w1. Access in 01/12/2019

COULDRY, N.; MEJIAS, U. **Making data colonialism liveable: how might data's social order be regulated?** Internet Policy Review, 8 (2). DOI 10.14763/2019.2.1411. 2019.

CUKIERMAN, H.L.; TEIXEIRA, C.; PRIKLADNICKI, R. **Um Olhar Sociotécnico sobre a Engenharia de Software**. RITA, v. XIV, n. 2, 2007.

DLA PIPER. **DATA PROTECTION LAWS OF THE WORLD, Full Handbook**. Available in: https://www.dlapiperdataprotection.com/. 2019.

ESCOBAR, A. **Designs for the Pluriverse: Radical Interdependence, Autonomy, and the Making of Worlds**. Londres: Duke University, 2018.

LATOUR, B. **Cogitamus: seis cartas sobre as humanidades científicas**. São Paulo: Editora 34, 2016.

__________ . **Reassembling the Social: An Introduction to Actor-Network-Theory**. Oxford: Oxford UP, 2005.

____________. **Science in Action: How to Follow Scientists and Engineers Through Society**. Londres: Open University Press, 1987.

MARQUES, I. **História das Ciências, Estudos CTS e os Brasis**. Abertura do IX Congresso Scientiarum Historia. Rio de Janeiro, 2016.

MEDINA, E.; MARQUES, I.; HOLMES, C. **Beyond Imported Magic. Essays on Science, Technology, and Society in Latin America**. EUA: MIT Press, 2014.

MOOR, J. **Why we need better ethics for emerging technologies. Ethics and Information Technology**. v. 7 (3), pp. 111–119. DOI 10.1007/s10676-006-0008-0. 2005.

PINTO, R. **SOBERANIA DIGITAL OU COLONIALISMO DIGITAL? Novas tensões relativas à privacidade, segurança e políticas nacionais**. Available in: https://sur.conectas.org/soberania-digital-ou-colonialismo-digital/. 2018. Access in 01/12/2019.

SCOTT, M.; CERULUS, L. **Europe's new data protection rules export privacy standards worldwide**. Available in: https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/. 2018. Access in 01/12/2019.

SOARES, G. **Rumo à governança algorítmica - análise sociotécnica dos algoritmos de credit score: o caso chinês**. XI Congresso Scientiarum Historia. Rio de Janeiro, 2018.

SUMPTER, D. **Outnumbered: From Facebook and Google to Fake News and Filter-bubbles – The Algorithms That Control Our Lives**. EUA: Bloomsbury Sigma, 2018.

ZUBOFF, S. **The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power**. EUA: PublicAffairs, 2019.