

# From Right to Written; An Inquiry into the Codification of a Right to Data Protection in Brazil

Roberto Sequerra Koogan Breitman

Thesis submitted for assessment with a view to obtaining the  
degree of Master of Arts in Transnational Governance of the  
European University Institute

Florence, [Click here to enter SUBMISSION date.](#)

European University Institute  
**School of Transnational Governance**

## From Right to Written; an Inquiry into the Codification of the Right to Data Protection in Brazil

Roberto Sequerra Koogan Breitman

Thesis submitted for assessment with a view to obtaining  
the degree of Master of Arts in Transnational Governance  
of the European University Institute

### **Supervisor**

Professor Madeleine De Cock Buning, EUI School of Transnational Governance

© Author, [Year] . This work is licensed under a [Creative Commons Attribution 4.0 \(CC-BY 4.0\) International license](https://creativecommons.org/licenses/by/4.0/)

If cited or quoted, reference should be made to the full name of the author, the title, the series, the year, and the publisher.

**Student declaration to accompany the submission of written work  
School of Transnational Governance**

I Roberto Sequerra Koogan Breitman certify that I am the author of the work *From Right to Written; an Inquiry into the Codification of the Right to Data Protection in Brazil* I have presented for examination for the Master of Arts in Transnational Governance. at the European University Institute. I also certify that this is solely my own original work, other than where I have clearly indicated, in this declaration and in the thesis, that it is the work of others.

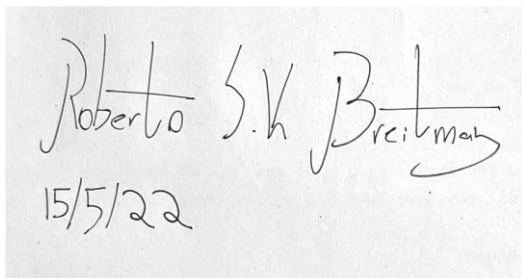
I warrant that I have obtained all the permissions required for using any material from other copyrighted publications.

I certify that this work complies with the Code of Ethics in Academic Research issued by the European University Institute (IUE 332/2/10 (CA 297)).

The copyright of this work rests with its author. Quotation from this thesis is permitted, provided that full acknowledgement is made. This work may not be reproduced without my prior written consent. This authorisation does not, to the best of my knowledge, infringe the rights of any third party.

I declare that this work consists of <10,009> words.

Signature and date:



Roberto S.K. Breitman  
15/5/22

## Abstract

This thesis analyses Brazil's *Lei Geral de Proteção de Dados*, and *Marco Civil da Internet* in an attempt to answer the question: "**to what extent is the right to Data Protection entrenched in Brazilian legislation?**". The investigation applies a black letter analysis approach to the laws, surveying the values at their foundation, the systems they put in place, and the procedural tools made available within that system. It concludes that while the values contained in the laws are consistent with a right to data protection, and the systems built give a strong framework for application, the right is jeopardized by a politicization of procedural tools.

## Table of Contents

<b>Abstract</b>	<b>5</b>
<b>Table of Contents</b>	<b>5</b>
<b>Introduction</b>	<b>7</b>
<b>Literature Review</b>	<b>9</b>
Data Protection in the Abstract	9
Data Protection as Opposed to Privacy	11
Data Protection as Reflecting Values	13
<b>Methods</b>	<b>17</b>
Approach	17
Document Selection	17
Scope & Limitations	18
<b>Data Protection in Brazilian Law</b>	<b>19</b>
Civil Rights Framework for the Internet	19
General Data Protection Law	22
Chapters 1-3	22
Chapters 4-5	24
Chapters 6-8	25
Chapter 9	26
Reflections	28
<b>Conclusion</b>	<b>31</b>



## Introduction

On February 10th 2022, Brazil's President Jair Bolsonaro signed into law constitutional amendment 115 'including a protection of personal data amongst the fundamental rights and guarantees' granted to Brazilian citizens.<sup>1</sup> The document is short, just four articles, adding Data Protection to the list of rights listed in the constitution, the list of competences given to the federal government, and stating these measures come into effect on the date of publication.<sup>2</sup> Nothing groundbreaking, as far as constitutional amendments are concerned.

What's interesting about this amendment is that it holds the distinction of being both expected, and utterly surprising. Expected because it comes at a moment where legislation on Data Protection has seen an uptick across the globe, with the European Union (EU) out in front and Brazilian legislation following close behind. Surprising because the president who signed the amendment, and has presided over the first two years of implementation of the country's flagship Data Protection law the *Lei Geral de Proteção de Dados* (LGPD), passed under his predecessor, is notoriously skeptical of any regulation of the internet, the realm where much of Data Protection legislation takes place.

In a speech accepting a communications award from his own communications ministry in 2021, Bolsonaro said in reference to internet use: 'We don't have to regulate that. We let people make themselves comfortable'.<sup>3</sup> This logic can be seen as malicious and at odds with Data Protection especially given Bolsonaro's track record on the issue. The day after the amendment was signed, Reuters reported on new federal police allegations of a targeted disinformation campaign being run by Bolsonaro's allies ahead of upcoming presidential elections in October 2022, just the latest in a series of investigations into online impropriety by the president and his cohort.<sup>4</sup>

Given this turbulent context, one must ask if the protections given in amendment 115 are being delivered by the government promising them. Understanding the current state of Data Protection in Brazil requires an inquiry into the laws that lie at its foundation; it is with that in mind that this investigation will work to answer the question "**To what extent is the right to Data Protection entrenched in Brazilian legislation?**". This will be done through a black letter analysis of the aforementioned LGPD along with its predecessor the *Marco Civil da Internet* (MCI),

---

<sup>1</sup> BRASIL. EMENDA CONSTITUCIONAL Nº 115, DE 10 DE FEVEREIRO DE 2022. Brasília, 2022. : <[http://www.planalto.gov.br/ccivil\\_03/constituicao/Emendas/Emc/emc115.htm](http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm)>. Acesso em: 7 Maio. 2022.

<sup>2</sup> ibid

<sup>3</sup> Bolsonaro, Jair. 2021. "Discurso Do Presidente Da República, Jair Bolsonaro, Na Solenidade De Entrega Do Prêmio Marechal Rondon De Comunicações- Palácio Do Planalto". Speech, Brasília, Brazil, , 2021.- Translation provided by author.

<sup>4</sup> Paraguassu, Lisandra, and Gabriel Stargardter. 2022. "Bolsonaro Allies Allegedly Pushing Fake News Effort, Brazil Police Document Says". *Reuters*. <https://www.reuters.com/world/americas/bolsonaro-allies-allegedly-pushing-fake-news-effort-brazil-police-document-says-2022-02-11/>.

relying on tools from scholarly and legal literature on the right to Data Protection for context and insight.



## Literature Review

This section will speak to the literature surrounding the issue at hand. The section will address literature on the right to data protection, considering work by legal scholars to understand exactly what right is being protected, and how that protection can be understood. This section will hope to set a foundation for the legal analysis that follows in the paper, ostensibly giving the tools to understand what goals Brazil's policy should aim to achieve.

The literature on Data Protection as a fundamental right has grown significantly in the past two decades as the prospect of defining and protecting that right became a political reality. This brief investigation will be organized as a downward trek through abstraction; starting with a look at the placement of key concepts and definitions, following that with a summary of two prominent theories, from which relevant tools can be pulled.

### Data Protection in the Abstract

Discussion of Data Protection as a right dates back to the 1970s, when theorists started to grapple with the implications of large data banks, and the forms of centralized personal data processing that came with them.<sup>5</sup> The right was immediately linked to the long standing notion of a right to privacy, with many early scholars arguing Data Protection ought be considered a subsection of that right rather than a right unto itself. Though that debate remains open, this paper will take the right's independence as a given due to its entrenchment in relevant legislation, and the strong body of scholarly work devoted to charting the relationship between these two rights.

Legal entrenchment can be seen in the European Union's recognition of the right in the Lisbon treaty, and in the Brazilian case through the adoption of constitutional amendment 115, both recognizing Data Protection as a fundamental right.<sup>6 7</sup> In scholarly terms, it seems well established that while Privacy is notoriously difficult to pin down, Data Protection's more procedural nature better lends itself to scholarly definition. The exact nature of that definition, and its conceptual relation to Privacy will be explored in the next sub-section.

The first major document to attempt codification was the European Union's Data Protection Directive (DPD), which defined the right as being concerned with protecting "the

---

<sup>5</sup> Bygrave, Lee A. 2002. *Data Protection law : approaching its rationale, logic and limits*. The Hague ; London: Kluwer Law International. Chapter 6, pages 93-123.

<sup>6</sup> European Union, *Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community*, 13 December 2007, 2007/C 306/01, available at: <https://www.refworld.org/docid/476258d32.html> [accessed 29 April 2022]

<sup>7</sup> Constituição Da República Federativa Do Brasil (1988), Emenda Constitucional Nº 115, De 10 De Fevereiro De 2022. Disponível Em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/Emendas/Emc/emc115.htm](http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm) . Acesso 29 de Abril 2022.

fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data”.<sup>8</sup> A similar definition can be found in the DPD’s successor, the European General Data Protection Law (GDPR), and in the first line of Brazil’s *Lei Geral de Proteção de Dados* (LGPD).<sup>9</sup> <sup>10</sup> The definition makes use of a key phrase found in the literature, ‘processing of personal data’, that should be defined to facilitate further analysis.

The processing of data can be understood as most forms of manipulation undertaken by the data’s holder, something Lee Bygrave describes as encompassing “the manner in which information is collected, registered, stored and disseminated”.<sup>11</sup> Acts that are covered by Data Protection when those data are *Personal*, meaning data that is either directly associated to, or allows the identification of an individual.<sup>12</sup> Bygrave explains this delineation as being rooted in principals of non-discrimination, the logic being that the processing of data that can be associated to particular individual could be used to that individuals disadvantage if not adequately regulated.<sup>13</sup> This reasoning, in turn, is premised on the observation that data processing is based on an inherent imbalance favoring the entity processing the data, over the subject that data is linked to. An advantage built on how modern technology removes limits on how much data can be stored, how that data can be manipulated, and for how long that data can be kept.<sup>14</sup>

It should be mentioned that while the definitions given above is used in the majority of scholarship, legislation, and jurisprudence, there are scholarly challenges, and grey areas can still be found at the margins. An example that illustrates these clashes can be seen in recent debates surrounding the use of cellphone metadata for law enforcement; the question being whether anonymized logs of locations, phone calls, and other activities are sufficiently identifiable to be protected. The issue has drawn meaningful debate around the world, as courts and scholars become increasingly concerned with the technical means by which seemingly innocuous sets of

---

<sup>8</sup>European Union, Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 24 October 1995, available at: <https://www.refworld.org/docid/3ddcc1c74.html> [accessed 29 April 2022]. Article 1 (1)

<sup>9</sup> Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Accessed April 30th 2022

<sup>10</sup> BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 2018. : <[http://www.planalto.gov.br/ccivil\\_03/\\_Ato2015-2018/2018/Lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm)>. Acesso em: 7 Maio. 2022.

<sup>11</sup> Bygrave 2

<sup>12</sup> ibid

<sup>13</sup> Bygrave 168

<sup>14</sup> Nissenbaum, Helen. “Protecting Privacy in an Information Age: The Problem of Privacy in Public.” *Law and Philosophy* 17, no. 5/6 (1998): 559–96. <https://doi.org/10.2307/3505189>.

information can be refined to the point of giving insights about the preferences and whereabouts of individuals.<sup>15</sup> The EU's highest court struck down legislation that mandated firms retain metadata so it may be available to law enforcement in 2014, Brazil's legislature went the opposite way (controversially) passing that same requirement in 2020, while the United States Supreme Court charted something of a middle path, issuing narrow restriction on the use of some metadata, in a 2018 decision.<sup>16 17 18</sup>

More substantive challenges to the concept of personal data processing as a whole can also be found, though they remain predominantly in scholarly circles. One prominent point, well voiced by legal scholar Nadezhda Purtova, is that as data processing becomes ever more ingrained in daily life, the notion of 'personal data' will grow to be so wide it is meaningless.<sup>19</sup> Purtova argues that twin increases in the amount of data collected, and the technical capacity to associate that data will make it such that most anything will become somewhat identifiable, meaning that regulation written to apply to specific cases will become the "law of everything".<sup>20</sup>

These types of debates are to be expected in implementing a new right, especially one so closely linked to rapidly advancing technology as Data Protection. That said, it is clear the field has matured to the point of having an established base (codified in law) that can sustain these criticism and questions as constructive rather than destabilizing. With that in mind, this investigation will use the mainstream definition of Data Protection as applying the processing of personal data. Doing so in the understanding that while valid questions and criticism exist, they have not yet significantly challenged that paradigm.

## Data Protection as Opposed to Privacy

The following two sections will seek to detail some prominent theories of data protection, meaning those theories that seek to go beyond particular facets of the right to explain its full logic, and relation to other understood rights. The first such theory to be seen was published by Paul De Hert and Serge Gutwirth in 2006, and has remained a relevant benchmark in the field; especially for its handling of Data Protection's relation to the right to Privacy.

---

<sup>15</sup> Bioni, Bruno, and Rafael Zanatta. 2020. "Levando Os Metadados A Sério". *Consultor Jurídico*. <https://www.conjur.com.br/2020-ago-13/bioni-zanatta-levando-metadados-serio>.

<sup>16</sup> Ni Loideain, Nora. 2015. "EU Law And Mass Internet Metadata Surveillance In The Post-Snowden Era". *Media And Communication* 3 (2): 53-62. doi:10.17645/mac.v3i2.297.

<sup>17</sup> Bioni and Zanatta

"Carpenter v. United States." Oyez. Accessed May 7, 2022. <https://www.oyez.org/cases/2017/16-402>.

<sup>19</sup> Purtova, Nadezhda (2018) The law of everything. Broad concept of personal data and future of EU Data Protection law, *Law, Innovation and Technology*, 10:1, 40-81, DOI: [10.1080/17579961.2018.1452176](https://doi.org/10.1080/17579961.2018.1452176)

<sup>20</sup> Purtova 40

De Hert and Gutwirth posit that Data Protection and Privacy ought be understood as fully separate legal tools within a democratic constitutional state, and that any confusion between them arises because the two often perform their separate roles simultaneously.<sup>21</sup> To the authors, these roles are best separated by the function they bring to the protection a citizen, with privacy being linked to a notion of *opacity*, while Data Protection is concerned with *transparency*. Opacity, they argue, are the tools used by governments to keep citizens free of unneeded or unwarranted interference; being implemented as a set of ‘normative choices about the limit of power’ allowed to society over individuals.<sup>22</sup> Transparency, on the other hand, dictates the parameters under which power operates within those limits. Being defined in the case of Data Protection as the tools used to ensure procedural fairness in the use of power to process data. In practice, these tools are largely complementary; as a judge asked to evaluate the legality of an act involving the processing of data would need to ask both if the processing constitutes a legal use of power (does it violate the lines set by opacity tools), and if that power was used in accordance with set legal standards (does it meet the bar set by transparency tools).

Though the logic inherent to this argument is sequential at the time of legislation, in that transparency rules are written for the protection of personal data only because it was determined that a there is a normative need to lift opacity in that field, It should be underlined that the theory does not consider Data Protection a subsection of privacy. In fact De Hert and Gutwirth celebrate the entrenching of a right to Data Protection as a needed codification of the limits of the right to privacy.<sup>23</sup> They recognize that ‘constitutional reasonableness encompasses substantive fairness *and* procedural regularity’, stating that too often privacy is invoked as a justification of both when it ought only be concerned with the former.<sup>24</sup> In that sense they greet Data Protection as the right concerned with the procedures that ought be used in the processing of personal data, seeing this as a substantive addition to the protections already granted by a right to privacy.<sup>25</sup>

As with any well respected theory, criticisms have been leveled against De Hert and Gutwirth’s conception of data protection. Maria Tzanou argues that in trying to separate privacy and data protection, the theory argues against itself. The logic being that if Data Protection holds a purely procedural role in evaluating how power can be used in the fields determined by privacy,

---

<sup>21</sup> De Hert, Paul, and Serge Gutwirth. "Privacy, Data Protection and law enforcement. Opacity of the individual and transparency of power." *Privacy and the criminal law* (2006): 61-104.

<sup>22</sup> De Hert and Gutwirth 70

<sup>23</sup> De Hert and Gutwirth 81

<sup>24</sup> De Hert and Gutwirth 103

<sup>25</sup> De Hert and Gutwirth 94

it marks itself as a luxury rather than a necessary right.<sup>26</sup> Put in terms of the original theory, her argument is that as long as the determining factor on whether an act is permitted is whether or not it falls within a field protected by opacity, all protections still flow from privacy. In her conception, the transparency tools brought on by Data Protection are good to have, but not essentially as they could be arrived at without the need for a separate right.<sup>27</sup>

This criticism is wise in pointing out that the right to Data Protection is much narrower than the right to privacy, given the latter encompasses all of a citizen's relations to those who would use their power to surveil them, while the former addresses only one specific instance of that power; however, this is not a reason to disregard the value of Data Protection all together. De Hert and Gutwirth's conception of transparency tools allows for them to be provided by other rights and systems when necessary, the value of their theory is in pointing out that Data Protection presents a specific case where their use is particularly relevant. Given the right to Data Protection arose from the observation that citizens face particular threats by the asymmetry created in the compiling and processing of personal data, a deliberate effort on the part of legislators to regulate how that processing is done seems both warranted, and necessary.

The strength of De Hert and Gutwirth's theory to an investigation such as this one is the clear prerogative it gives to Data Protection legislation. This paper will take from this theory by recognizing two principal goals for sound laws entrenching this right. The first is that Data Protection laws must acknowledge the space in which they operate, meaning they must clearly state what part of the normative determination for lifting opacity they seek to address. It is here that the notion of Data Protection as being concerned with the *processing of personal data* is useful, as it provides a legal term whose definition (even if contentious or as yet incomplete) can be used to draw the boundary for the applicability of the law. The second is that these laws should give practical, applicable standards for the evaluation of actions taken within the boundaries they set. Given data protection's role as a guarantor of 'procedural regularity' its principal aim should be to outline that procedure in ways that facilitate compliance and create the possibility for recourse should transparency parameters not be met.<sup>28</sup>

## Data Protection as Reflecting Values

Where the previous theory sought to define the right Data Protection in terms of the tools it grants in the protection societal values, the second launches its explanations from an attempt to outline the values addressed by the right. The theory, authored by Yvonne McDermott, prefaces

---

<sup>26</sup> Tzanou, Maria, Data Protection as a Fundamental Right Next to Privacy? 'Reconstructing' a Not so New Right (May 1, 2013). International Data Privacy Law, 2013, Vol. 3, No. 2, pp. 88-99, Available at SSRN: <https://ssrn.com/abstract=3076415>

<sup>27</sup> Tzanou

<sup>28</sup> De Hert and Gutwirth 102-103

its analysis by acknowledging that “the point” of fundamental rights protection is to “reflect the norms underpinning a legal order”, meaning one should be able to distill those values out of existing legislation.<sup>29</sup> The paper goes on to do just that, naming and interpreting four key values addressed by Data Protection laws: Privacy, Autonomy, Transparency, and Non-Discrimination.

McDermott does not offer comment on the relation between the rights to privacy and Data Protection (though the existence of both is acknowledged), choosing instead to focus on on data protection’s role in protecting privacy as a value.<sup>30</sup> The author outlines the value as existing on several levels, with Data Protection being concerned with the most abstract of those conceptions; namely that of privacy as the “protection of one’s identity”, a notion the paper credits to Hildebrandt.<sup>31</sup> Though some nuance is offered, like the acknowledgement that the protection of certain data (health data) might fall under narrower conceptions like a ‘reasonable expectation of privacy’, the connection between Data Protection and privacy is taken almost as a given in the paper.

Significantly more attention is given to the rights relation to Autonomy. The author pulls this value from the centrality of consent as a mechanism in Data Protection legislation, arguing that it had been the intention of those drafting these laws to grant citizens increased control over how their data is processed. McDermott notes that while this goal is clear, there is still debate as to what conception of autonomy is being addressed by legislators and jurists, with two principal contenders bearing mention. The first comes from a decision by German courts establishing the notion of ‘informational self determination’, meaning a persons right to determine how their data is disclosed or used, mandating ‘clearly defined conditions of processing’, and emphasizing that individuals should not be ‘reduced to a mere object of information’.<sup>32</sup> To McDermott this reading signals the use of a ‘will theory of rights’, whereby a rights holder may subject others to the obligation to respect that right.<sup>33</sup> This line of inquiry is especially interesting to this thesis, as the term ‘informational self determination’ can be seen translated into Portuguese (*‘autodeterminação informativa’*) as the second listed fundamental goal of the LGPD, an observation that will be further explored in in a later section.<sup>34</sup>

---

<sup>29</sup> McDermott, Yvonne. “Conceptualising the Right to Data Protection in an Era of Big Data.” *Big Data & Society*, (June 2017). <https://doi.org/10.1177/2053951716686994>.

<sup>30</sup> McDermott 3

<sup>31</sup>Hildebrandt M (2006) Privacy and Identity. In: Claes E, Duff A and Gutwirth S (eds) *Privacy and the Criminal Law*. Oxford, UK: Hart, pp. 43–60. (As cited by McDermott, 3)

<sup>32</sup> Volkszählungsurteil, 16 BVerfGE 1, 68-69 (1983). (As cited by: Tzanou, 89)

<sup>33</sup> McDermott

<sup>34</sup> BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD) art.2, II. Brasília, 2018. : <[http://www.planalto.gov.br/ccivil\\_03/\\_Ato2015-2018/2018/Lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm)>. Acesso em: 7 Maio. 2022.

The second reading of autonomy recognized in the theory is described as being seen in requirements in the EU's General Data Protection Act that data controllers take certain measures to protect an individual's data regardless of whether that individual has requested those measures. This is seen as being consistent with an 'interest theory of rights', which sees human rights as 'imposing a positive duty actors to respect the interest of others' even if no claim to that right has been made.<sup>35</sup> The core question brought on by this distinction is whether citizens ought need to assert their right to autonomy over their data in order to have it protected, weighing governments interest in allowing its citizens greater freedom, against its role as a protector of citizens interests. McDermott falls on the side of increased government protection, meaning an interest theory of rights. They argue that given most citizens are unaware of the level of data collection and processing done, and thus would not know to assert their right, placing obligations on data holders is 'both proportionate and necessary'.<sup>36</sup>

The next value McDermott sees as tied to Data Protection is Transparency. Not much needs to be said here, as the text directly calls on De Hert and Gutwirth's conception of transparency as operationalizing the use of 'normatively accepted power'.<sup>37</sup> The meaningful addition made to that framework here is how this theory links that power to objective mechanisms in Data Protection law, pointing to how the GDPR defines and parametrizes consent in the context of data processing; pointing to sections requiring that requests for user consent should be easily read and understood by users as an example of standard setting.<sup>38</sup>

Finally, the theory links Data Protection to another usual suspect, non-discrimination. The connection made by McDermott is similar to what was noted by Bygrave in describing the need for regulating the processing of personal data: that this processing could be used to profile and disadvantage the individual that data describes. McDermott points to provisions describing limits to data processing and storage as concerned with protecting a persons 'future life' in that the disadvantages from processing may come long after the data was collected.

In the context of this thesis, the greatest strength of McDermott's work is also its greatest weakness. Since the theory derives its characterization of the values addressed by the right to Data Protection from an inductive analysis of existing legislation, it is limited by both the authors personal assessment of what regulations are relevant and what is relevant in each regulation. That said, given the body of law on the matter is fairly robust in Europe, and the paper has been well received in academic circles, it fair to say the values McDermott recognizes can be taken as signifiers of the values underpinning particular forms of regulation for data protection. In this

---

<sup>35</sup> McDermott

<sup>36</sup> McDermott

<sup>37</sup> McDermott

<sup>38</sup> McDermott

investigation, these connections will be a useful tool for assessing goals in legislation, as will be done in subsequent sections.



# Methods

## Approach

The question at hand is of a strict legal nature. With this in mind, this investigation will employ a purely legal method, namely Doctrinal Analysis. Also called Black Letter analysis, this a method that takes into account the contents of law, or set of laws analyzing them measure by measure with the objective of arriving at an understanding of the system, or idea they describe.<sup>39</sup> In the case of this investigation this method will be applied to two documents, the *Marco Civil da Internet* (MCI), and the *Lei Geral de Proteção de Dados* (LGPD). They will be analyzed against the standards set in the literature, in an attempt to answer the research question. This method allows for rigorous engagement with the selected documents, giving the opportunity for meaningful insights to both the underlying values of the law, and the mechanisms made available for actualizing those values.

Though these considerations are strictly secondary, other sources were also consulted in an effort to contextualist the laws within Brazilian history, and as a means of adding color to eventual conclusions. Additional sources include a selected set of primary source, including speeches by relevant law makers, and secondary sources, including government press releases and newspaper articles. These are reserved for sections concerned with contextualization and overarching analysis, and an effort has been made to flag these sources as commentary on this pieces principal conclusions.

It should also be mentioned that while the method of analysis used here is purely legal, many of the observations and conclusions arrived at may be political in nature. This is to be expected given the contentious nature of Data Protection legislation in Brazil, and an effort has been made to demarcate the legal from the political in the analysis.

## Document Selection

The MCI and LGPD were selected as the principal sources for this investigation due to their preeminent position in the Brazilian legal cannon as concerns a right to Data Protection. A third candidate comes to mind in this context: Constitutional Amendment 115 mentioned in the introduction to this paper. That document will not be treated alongside the other two, as where the MCI and LGPD are substantive pieces of legislation aimed at entrenching a right to data protection, the amendment is a short document simply adding the right to the national constitution. Given this investigations focus on the systems put in place, this laws symbolic nature would add little to no new information to the investigation.

---

<sup>39</sup> Andria Naude Fourie, "Expounding the Place of Legal Doctrinal Methods in Legal-Interdisciplinary Research," *Erasmus Law Review* 8, no. 3 (December 2015): 95-110

## Scope & Limitations

This investigation seeks to understand the underlying strength of system entrenching Data Protection in Brazilian law, not to critique or analyze the particular decisions that make it so. As such, the scope of this investigation includes sections of the laws concerned with values and the granting of rights, along with sections devoted to building systems that allow these values to be implemented. Notably, this scope excludes deep analysis of particular marginal decisions made in that system. As such, aspects like the exact value of fines, or the exact requirement for consent to data processing will be relevant in their presence, but analysis will not extend as far as questioning the the exact numeric values, or standards used.

Finally, two principal limitations bear mentioning. The first is concerned with the nature of the method used. It's often said that analysis focusing exclusively on the letter of the law risks losing the nuances of how that law is received in society. This is certainly a risk in this investigation, and it was with this in mind that contextualizing sections, and sources were added to supplement the role of pure legal analysis. It must be acknowledged, however, that these measures can only go so far, so it is important to note that the conclusions drawn here are relevant to the Brazil's legal framework, and the societal applicability of these laws should be the subject of a subsequent inquiry.

The second limitation is relevant to the literature used in completing this analysis. It should be noted that the majority of the authors and cases listed in the literature review are concerned with laws and jurisprudence of Data Protection in Europe. These were chosen as Europe is a global leader in Data Protection and, as will be seen, because Brazil has openly taken many cues from the European system. All the same, it must be noted that departure from that model is not necessarily a bad thing, and thus care has been taken to flag differences between the Brazilian and European approach as 'departures' rather than mistakes.

## Data Protection in Brazilian Law

The right to Data Protection in Brazil can be thought of as occurring in two acts, taking place under the auspices of three presidents. This section will analyze each of two laws, while considering the political context in which they were written in an attempt to understand the state of Data Protection in Brazilian legislation today. Investigation will start with a look at the Rousseff administration, centering on the *Marco Civil da Internet* (Civil Rights Framework for the Internet), move to deep study of the *Lei Geral de Proteção de Dados* (General Data Protection law) passed under president Michel Temer, with brief mention of the implementation of that law under President Jair Bolsonaro.

### Civil Rights Framework for the Internet

Brazil's Civil Rights Framework for the Internet (MCI) was passed into law in April 2014, championed by president Dilma Rousseff of the *Partido dos Trabalhadores* (Workers party).<sup>40</sup> The law was written by the office for legislative affairs in the Justice Ministry of then president Luiz Inácio Lula da Silva (also of the Workers Party) in 2009 under advice from the Brazilian Internet Steering Committee (CGI.br), and the members of the law faculty at the Fundação Getulio Vargas (FGV).<sup>41</sup> It was presented to the national congress in 2011, but was only brought to a vote in 2013 following disclosures by Edward Snowden of widespread illegal espionage conducted by the United States of America.<sup>42</sup> The disclosures included confirmation that the United States government has spied on Brazilian institutions, including high ranking government officials. Rousseff called the act a "violation of fundamental rights" in an address to the United Nations General Assembly, and linked it to MCI's passing through the legislature in 'record time' in her opening address at the NET Mundial conference in 2014.<sup>43 44</sup>

---

<sup>40</sup> BRASIL. Marco Civil da Internet. Lei 12.964/14. Disponível em: < [http://www.planalto.gov.br/ccivil\\_03/ato2011-2014/2014/lei/l12965.htm](http://www.planalto.gov.br/ccivil_03/ato2011-2014/2014/lei/l12965.htm) >. Acesso em: 11 de maio 2022

**Note:** this law will be mentioned extensively in this section, with readability in mind, those citations will be handled in text. All translations from Portuguese are offered by the author.

<sup>41</sup> "O CGI.Br E O Marco Civil Da Internet". 2014. *CGI.Br - Comitê Gestor Da Internet No Brasil*. <https://www.cgi.br/pagina/o-cgi-br-e-o-marco-civil-da-internet/>.

<sup>42</sup> Rousseff, Dilma. 2014. "Discurso Da Presidenta Da República, Dilma Rousseff, Durante Cerimônia De Abertura Do Encontro Global Multissetorial Sobre O Futuro Da Governança Da Internet". Speech, Net Mundial, Sao Paulo, SP, 2014.

<sup>43</sup> Rousseff, Dilma. 2013. "Statement By The H.E. Dilma Rousseff, President Of The Federative Republic Of Brazil, At The Opening Of The General Debate Of The 68Th Session Of The United Nations General Assembly". Speech, New York, , 2013.

<sup>44</sup> Rousseff, Net Mundial

With this context in mind, one can expect the resulting legislation to pay particular attention to codifying existing notions of fundamental rights as pertains to internet activity, with particular attention being given to privacy. This expectation is bourn out in a reading of the document. Chapter 1 sets out the law's 'preliminary dispositions', stating in its first article that it is concerned with the 'rights and duties for the use of the internet in Brazil' (ch.1 art.1). Of these objectives, terms relevant to Data Protection can be found in article 3. The article lists the 'principles' at play in the use of the internet, marking the 'protection of privacy' and the 'protection of personal data' amongst them (ch.1 art.3 II,III). It also states that agents ought be held responsible in accordance with their activities, a notion that creates space for recognizing differing roles of data holders and data owners in online interaction. The rest of the chapter speaks to access to the internet, the laws relation to other statutes on telecommunications, and definitions of internet governance terms, none of them directly relevant to data protection.

The concepts in chapter one are interesting for two reasons. First, the distinction made between privacy and Data Protection indicates an understanding that these principles are distinct; whether that distinction will go along the normative/practical divide proposed by De Hert and Gutwirth is yet to be seen.<sup>45</sup> Second, the division of online actors by activity shows an understanding by law makers that actors on the internet exist on different footing, it is a necessary observation for recognition of the potential discrimination and power asymmetries that a right to Data Protection aims to correct.<sup>46</sup>

Concerns for the wellbeing of data owners can be seen in chapter 2 of the Civil Rights Framework for the internet, which is concerned with 'rights and guarantees to users', more specifically in its lengthy 7th article (ch. 2). The article lays out a list of rights to be guaranteed to internet users, many of which echo principles seen in the McDermott's work on the values linked to data protection.<sup>47</sup> In the guarantee that a users data will not be shared with third parties (ch. 2 art.7 VII), one can see a concern for user's 'future life' consistent with a notion of self-determination in that users as assured that data shared with a particular entity will not surprise them in a later separate occasion. A similar case can be made for the guarantee of the 'definitive exclusion of personal data' by a particular web application provider at the end of their relation with a user (ch. 2 art.7 X). This section can be read as a nod to the the autonomy, as it bolsters a users agency in choosing to terminate their relation with those who hold their data.

A second strain of values can be found in the rights given by chapter 2 article 7 in provisions detailing a users rights relevant to the collection, storage and processing of their personal data. These include the right to 'clear information' on the reason for data collection, and

---

<sup>45</sup> De Hart and Gutwirth 103

<sup>46</sup> Bygrave

<sup>47</sup> McDermott

the legality of that collection in all applications' terms of service (ch.2 art.7 VIII). A protection bolstered by the requirement that collection only be carried out with the consent of the user, with clauses relevant to that consent being required to be highlighted amongst other contractual clauses (ch.2 art.7 IX). These fall squarely in the set of measures the literature would link to Transparency. They indicate a first step towards the types of procedurally useful tools described by De Hert and Gutwirth, though given their modest scope, they are likely best thought of as a reflection of transparency as a guiding value. Article 7 accounts for most of the chapter two, with the remaining provisions being concerned with users access to the internet.

Chapter three, section two contains the last of the MCI's provisions relevant to data protection. The chapter is concerned with the 'provision of connection, and applications on the internet', and its second section specifically with the 'protection of registries, personal data and private communications' (ch.2 sec.2). While the title includes data protection, the content makes it clear that this is meant as the security of data not the full right to Data Protection being discussed. Article 10 provides that holders of personal data will only be obligated to turn over these facts if served with a judicial order (ch.2 sec.2 art.10). Article 11 speaks to jurisdiction, stating that all data and private communication collected, stored, or treated in Brazilian territory are subject to Brazilian law (ch.2 sec.2 art.11). Finally, article 12 provides guidelines for penalizing infractions to the measures given in the previous two, with potential consequences including warnings, fines, and judicial orders to suspend or prohibit acts inked to the infraction (ch.2 sec.2 art.12).

The measures given in chapter three are particularly relevant to this investigation as they are the first instance of the types of procedural legal tools de Hert and Gutwirth describe as being the principal function of the right to data protection.<sup>48</sup> That said, the fact that these legal penalties are only applicable to the measures contained in the chapter underlines how the Civil Rights Framework for the Internet is not intended as a full implementation of the values it sets out.

On the whole, while the MCI can be seen to make interesting nods to data protection, it is hard to think of it as meaningful legislation to entrench that right. The document does not give many specific procedural measures for enforcement, a crucial feature of Data Protection legislation, instead sticking to the granting of specific rights. This is consistent with its stated objective of giving a foundation to future legislation on internet governance. In that sense, the document is likely best seen as a political artifact; a piece that sets Brazilian law on path consistent with the principles and ideas associated with a right to data protection. The importance of such an artifact should be understated, as though it may not offer a full direct claim to the right, it sets and accelerates the agenda for future legislation.

---

<sup>48</sup> De Hert and Gutwirth

These observations are shown to be salient when considering the law in political terms. Discussion within the Brazilian legislature that started with the expedited passing of the MCI commonly saw the framework as a leading up to a broader law.<sup>49</sup> Efforts to write that law gained steam as public consultation project began in 2015 under leadership of the office for consumer protection in the Justice Ministry, which revised an existing draft law. The law was important the Rousseff administration (then in its second term), as evidenced by the project being sent to the congress as a legislative priority in may of 2016, the day before she was removed from office (Rousseff was eventually impeached). The remainder of Rousseff's term was passed to vice-president Michel Temer of the center left *Movimento Democrático Brasileiro* (Brazilian Democratic Movement), who removed the priority tag, but continued developing the law. The LGPD was passed in 2018, and stands as the preeminent document on Data Protection in Brazil.

## General Data Protection Law

The LGPD is a broad law aimed at implementing a system for regulating the processing of personal data in Brazil.<sup>50</sup> Given this wide scope, this investigation will divide the document's 9 substantive chapters into thematic clusters for ease of analysis. Chapters 1-3 speak to the laws principals, and rights granted to citizens. Chapters 4-5 provide an interface between those rights and the Brazilian government. Chapters 6-8 detail the mechanisms by which these rights are to be implemented. Finally, chapter 9 details the creation of a new government body, the *Autoridade Nacional de Proteção de Dados* (ANPD), or National Data Protection Authority. An Additional section will be included to address the document as a sum of its parts, and give a brief look to its implementation thus far.

At this point it is relevant to restate that while this investigation is interested in the existence of systems to implement a right to data protection, and how these systems are entrenched, it is not the objective of this thesis to examine the specific ins and outs of these systems. This distinction was moot when looking at the MCI as its concerns are predominantly ideational, but comes into play in the LGPD as it is significantly more procedural.

### CHAPTERS 1-3

The first three chapters of the LGPD form its ideational core. As can be expected, chapter 1 is concerned with the laws preliminary dispositions; its first article stating the law speaks to the

---

<sup>49</sup> Roncolato, Murilo. 2015. "Por Que Debater A Lei De Proteção De Dados Pessoais? - Link - Estadão". *Estadão*. <https://link.estadao.com.br/noticias/geral,por-que-debater-a-lei-de-protecao-de-dados-pessoais,10000029762>.

<sup>50</sup> BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 2018. : <[http://www.planalto.gov.br/ccivil\\_03/\\_Ato2015-2018/2018/Lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm)>. Acesso em: 7 Maio. 2022.

**Note:** this law will be mentioned extensively in this section, with readability in mind, those citations will be handled in text. All translations from Portuguese are offered by the author.

'processing of personal data, including through digital means' this a meaningful addition for what is not written, namely that this law extends beyond data exchanged through the internet as was the case in the MCI (ch.1 art.1). This notion is further specified by article 4, which lists cases of processing that are not addressed by the law (ch.1 art.4). These include processing for purely personal reasons, purely artistic or journalistic reasons, and in certain cases for national security (ch.1 art.4). Though limiting to the right to data protection, the explicit statement of these exceptions ought be read as an indicator of the laws strength - As De Hert and Gutwirth emphasized, the right to Data Protection depends on a clearly defined normative distinction of their scope.

Article 2 speaks to the principals the law seeks to protect, giving a list similar to the one seen in the MCI with the notable addition of 'consumers rights' and 'informational self-determination'. Both values are consistent with the literature, as a pivot from a telecommunications angle to a consumer rights angle indicates recognition of the types of asymmetries Bygrave placed at the core of the right to data protection, and 'informational self-determination' appears to be a term borrowed from he German court ruling McDermott pointed to as a key in actualizing a protection of autonomy.<sup>51 52</sup> This trend continues into article 5, which gives relevant definitions (ch.1 art.5). Here one finds voicing of both 'processing' and 'personal data' nearly identical to what the literature recognizes as standard in the EU. There is the notable addition of a special subcategory for 'sensitive personal data', described as data pertaining to ones ethnic or racial origin, religious or political preference, along with health data and sexual orientation; a measure seemingly aimed at granting extended protection to data that might be used to discriminate.

Chapter 2 speaks to the requirements for the processing of personal data, its first section centering on the notion of consent. The law states that consent is required for data processing, with some few exceptions being listed in article 7. Consent is then defined in article 8 as requiring positive statement from the user (written or otherwise), having to be specific to the data processing being carried out (a notion expanded on in article 9), and nullifying any coerced, or overly broad documents (ch.2 art.8). These measures are similar in spirit to those seen in the MCI, but give more specific language to the requirement, making it a stronger procedural tool for data protection.

The two sections that follow in chapter 2 detail the additional protections given to sensitive personal data (ch.2 sec. 2), and specific rules for the processing of data belonging to underage citizens (ch.2 sec. 3). Both state their protections in terms of consent, with article 11 requiring explicit added consent for the processing of sensitive personal data, in the exception that this data be indispensable for certain very limited purposes, such as the legal obligation given by this

---

<sup>51</sup> Bygrave

<sup>52</sup> McDermott

law, the exercise of the users rights, or saving a life. Articles 12 and 13 follow in the vein of limiting the use of sensitive data, placing higher standards for the anonymization of these data, and their use in public medical studies. Section three gives particular measures on processing the data of underage people. As can be expected, the law requires this consent be given by the child's parent or guardian, though it interestingly also requires that consent to processing not be a required step to accessing games or online applications unless the data disclosed is of necessary importance to the application. These additions further entrench the use of consent as a tool for deciding the applicability of the law; narrowing it to the point of judicial usefulness.

Chapter three, the last in this set, is concerned with the rights of data holders. There is little to say here, as this chapter closely mirrors chapter 2 of the MCI with a few additions, chief amongst them an expanded set of provisions aimed empowering data owners to understand what data is being held, how its being used, and if needed, to correct the record. Unlike the narrow language used in the previous chapter, these rights are given in abstract terms, with the promise that they ought be fulfilled in accordance with 'legislative systems that follow' (ch.3 art.18).

Chapters one through three successfully play a double function: laying out values for Data Protection legislation in Brasil, and outlining where that legislation applies. The values given in chapters one and three extend on the work started in the MCI, enshrining strong definitions consistent with relevant scholarship, extending the scope of protection to cover the processing of all personal data, and tying relevant values to meaningful tools. Chapter two takes those definitions, and gives them procedural weight by wading into the nuances of application. Through an exploration of consent, the chapter builds a meaningful framework for evaluating the applicability of the law, exceptions and all. Put in terms of the scholarly literature used in this analysis, these chapters represent the completion of the enterprise of normative definition that began in the MCI; making use of Opacity tools to define the scope of data protection.<sup>53</sup> Keeping with the scholarly framework given by De Hert and Gutwirth, the next step is to see how transparency tools are used to manage the space outlined here - this is where Data Protection should show its teeth.

## **CHAPTERS 4-5**

The effort to codify protection starts with chapters on government processing of personal data, and the international transfer of data. The former is the topic of chapter four, which essentially serves as a mapping of other provisions given in the law to government, and to existing legislation, while the later gives rules dictating that personal data can only be exported by data holders in particular circumstances, and to countries that meet minimum Data Protection levels; the nuances of which are not within the scope of this investigation.

---

<sup>53</sup> De Hert and Gutwirth



Two points that do raise interest, are article 29 and section 2 of chapter 4. Article 29 states that the National Data Protection Authority (ANPD) is empowered to request reports on data processing from any public body, and give further instruction to ensure the LGPD is followed (ch.3 art.29). This is similar to what is seen in section two, which is concerned with the 'responsibilities' of government. The section very short, only 5 lines long, and its two articles state that infractions of the LGPD by government will be handled by the ANPD (ch.3 sec.2 art.31), and that the ANPD will be empowered to mandate the publishing of reports on Data Protection in government, and issue standards (ch.3 sec.2 art.31). These two sections are notable, in that instead of giving tangible mechanisms by which violations will be dealt with, the law delegates to the ANPD. This dynamic puts meaningful power in the hands of that organization, essentially making the strength of Data Protection in the government dependent on the strength of the National Data Protection Authority.

## CHAPTERS 6-8

These chapters contains the meat of the legislations, mandating the creation of roles within data holding firms charged with data protection, the security and best practices they should apply, and speaking to sanctions for failures to do so. Again, the nuts and bolts of this system are not the strict focus of this paper, but a brief overview is useful. The system called for by the LGPD is broadly similar to that of the EU's General Data Protection Law, an influence acknowledged by both the EU and the laws authors.<sup>54</sup> Like its European cousin, the Brazilian law requires firms of a given size appoint, and publicly name, a 'data controller' who is made responsible for decisions and procedures on data processing (ch.6 art.37), and a 'data operator' who answers to the controller and is responsible for actually processing the data (ch.6 art.37); both of whom may be held legally responsible for harms to data owners. Notably, the LGPD requires both roles be present in all relevant firms, while the GDPR allows for processing without an appointed operator under certain circumstances.<sup>55</sup> The controller and operator, once named, are required to announce and follow a set internal rules and best practices for the handling of personal data that are to be consistent with the principals and rights given by the LGPD. Failure to comply with these guidelines, or breaches that cause harm to data owners are subject to investigation and eventual fines or sanctions, again similar in structure to both the GDPR and the MCI.

Like in the previous section, one aspect of these chapters that raises concern is the amount of necessary regulation that is left to the ANPD rather than being included in the body of the law; a clear departure from the GDPR, which envisions no such agency. These responsibilities can be thought of in three sections, the first being the agencies role in setting guidelines for best practices. Article 46 calls on the National Authority to provide 'technical standards' for minimum

---

<sup>54</sup> "What Is The LGPD? Brazil'S Version Of The GDPR - GDPR.Eu". 2022. *GDPR.Eu*. <https://gdpr.eu/gdpr-vs-lgpd/>.

<sup>55</sup> *Ibid*

measures that ought be taken in developing procedures in respect to the LGPD's objectives (ch.7 art.46), with subsequent measures charging it with overseeing the eventual codes used (ch.7 art.50 II). Given the fast changing nature of technology and processing methods, one can see why it makes sense to have the standards for processing practices in the hands of a dynamic organization rather than entrenched in static law. That said, these procedures are the direct interface between the LGPD's values and the real processing that will go on in Brazilian firms, and thus represent a large section of the transparency tools mentioned by De Hert and Gutwirth. Placing these powers in the hands of the ANPD make the agency the key actor in determining the eventual strength of the LGPD as a whole.

The second role given to the ANPD is in receiving and processing reports of data breaches. The national Data Protection Authority is called upon to determine what constitutes a reasonable time frame for reporting, and once a report is filed, determine whether it ought be made public, and what mitigatory measures ought be taken by the data controller (ch. 7 art. 48). These measures give the ANPD the character of an oversight agency, concerned not only with the standards set, but also the particulars of individual implementation cases.

The final role given to ANPD is as an issuer of administrative sanctions, an expansion of its role as a case-by-case oversight agency. These provisions are given in chapter 8, which details a set of possible sanctions, leaving the job of creating a schedule for their use in the hands of ANPD. Article 53 states that this schedule will be written with public consultation, and be issued under the agencies own 'regulatory power'. While the power to instruct data controllers on managing breaches constitutes an oversight role, the creation of a penalty schedule and the determination of a timeline for reporting ought be seen as a legislative competence. Again, there may well be benefit to having these powers in the hands of a dynamic organization, but flaws in the creation of this material, or failure to issue them could make the LGPD outright unenforceable, as it would deprive practitioners of the tools needed to make rulings on relevant cases. This is especially true of the reporting guideline, as it is conceivable that a case would be brought by a private citizen if a firm fails to report a relevant breach.

In terms of the provision of a right to data protection, chapters 6-8 of the LGPD present a strong system based on a well received model, but the laws departures from that model present variance. If well implemented, the ANPD is positioned to become a staunch defender of Data Protection rights, equipped with the tools needed to adapt protections to fit a changing field. However, if the ANPD is unable or unwilling to complete this role, it can weaken or even nullify the laws effectiveness. This dynamic makes clear that the procedural portion of Data Protection will not be guaranteed in the body of the LGPD, rather analysis must turn to the systems that may help or hinder their implementation through the ANPD.

## CHAPTER 9

Having placed it at the heart of the right to data protection, the LGPD turns to defining the National Data Protection Agency in its 9th chapter. These regulations are different from all that have been seen thus far, in that instead of speaking to values and their embodiments, it defines a legal body setting paradigms for its creation and operation. Given the importance of the ANPD to the strength of Data Protection in Brazil, this section will delve into those nuances using both legal and political analysis to gage the strength of the body being described.

The chapter's first article, article 55-A, creates the ANPD as a body for public administration and a member of the executive branch of the Brazilian federal government. The body is to hold that status for not longer than two years, at which point the executive will see it transformed into a body 'submitted to a special autarkic regime linked to the presidency of the republic' (ch.9 art 55-A). The relevance of this measure is largely budgetary, essentially stating that the ANPD will be directly dependent on the executive's budget for up to two years, before being given greater autonomy through funding streams described later in the chapter. Actions such as these are common in the creation of new public bodies, but raise critical political questions in the specific case of the ANPD; in that large parts of its power are expressed throughout the guidelines and regulations it will likely produce in the first years of its existence. Though these policies may be changed later, the creation of the agency is a critical juncture from which the path for the right to Data Protection will be set. That this phase will be characterized by direct financial dependence on the executive grants whatever administration is in power during that period meaningful sway over the direction the agency, and the right to data protection, will take.

Article 55-B guarantees the organizations 'technical and decision-making autonomy', an encouraging prospect, though the question must be asked - decision making by whom? The rest of the chapter is concerned with the organizations internal structure, powers, and responsibilities. Article 55-C establishes the authorities constituent bodies, chief most them being the a Directing Council as the organization's top body, and a 'National Council for Data Protection and Privacy'. The Directing council is to be composed of five members, amongst them a Director-President, all appointed by the President of the Republic and subject to confirmation by the senate for 4 year terms (ch.9 art. 55-D). Similar rules are given for removal of a council member, which occurs only through resignation, judicial action, or termination by the president of the republic; who is also charged with nominating a replacement to complete the outgoing council member's term (ch.9 art. 55-F). This council is charged with leading and organizing the ANPD's staff in completing all the initiatives mentioned in the previous section, meaning they will be the ones empowered to make legally enforceable guidelines for data protection, receive and process data breach reports, and issue appropriate sanctions (ch.9 art. 55-J).

If the monetary situation gave the executive sway over the ANDP, the structuring of the Directing Council gives it outright control. Having the terms of council members coincide with presidential terms (also four years) shows that the roles are designed to be political in nature; changed by incoming administrations without the need to deliberately fire their predecessors

choice. The paradigm created by this design is at odds with the language seen earlier in the document, as what is described as a stable right to Data Protection is subject to the whims of political change; more a lever of power than a right.

This political streak is less pronounced in the make up of the National Council for Data Protection and Privacy. The council is composed by 23 members, who serve two year terms, and are nominated by a variety of relevant sectors, as prescribed in article 58-A. The largest single share is given to the executive, with five members, another five are distributed amongst government bodies, including one from each legislative house, and three from relevant agencies (ch.9 art. 58-A). The remaining thirteen are distributed between academia, industry, and labor rights organizations, with no single entity holding more than three seats (ch.9 art. 58-A). This body is charged with proposing strategy to the Directing council, writing an annual report on the ANPD's actions, and holding public consultation when called to do so (ch.9 art. 58-B). The inclusion of a multi-sectoral body at the heart of the ANPD is an encouraging prospect, though it is blunted by the council's predominantly advisory role, and the amount of representation given to government appointed officials. The body may well bring useful insights to the ANPD, serving as a conduit for observations on Data Protection from relevant stake-holders, though the extent of its function will remain dependent on the Directing Council's willingness to accept suggestion.

Assessing the ANPD's effect on Data Protection in Brazil brings no final answers; instead one must contend with the element of chance that comes with the politicization of what was described as a fundamental right. As was already seen, the ANPD's responsibilities add up to majority of the transparency tools described in the literature as the principal concern of a right to data protection.<sup>56</sup> It is now clear that those responsibilities are not carried out in the LGPD itself, as though the framework put in place in chapters 6-8 is sound, the ANPD is given a wide berth on if and how it will make use of the those systems. From reading chapter 9 one can surmise that the strength of Data Protection tools will swing on political decisions, owing to the clear control exercised by the executive over the organization.

## **REFLECTIONS**

All things considered, the LGPD should be taken as a long stride towards entrenching a right to Data Protection in Brazil, though it doesn't finish the job. Chapters 1-3 set up a strong foundation for protection of the right; using established, specific definitions and showing a willingness to delve into the nuances of applicability through the principal of consent. The section establishes most the principals cited in the literature for a strong version of a right to data protection, giving citizens salient rights and giving jurists space to apply those rights. The section addresses the normative bounds of the law, creating a well delineated space for a system to fulfill its stated aims.

---

<sup>56</sup> De Hert & Gutwirth

Chapters 4-5 and 6-8 do the heavy lifting in creating that system, taking cues from Europe's GDPR to build an interface through which government can impose controls, standards, and sanctions on data holders on behalf of data owners. Put in De Hert and Gutwirth's language, these sections scan the normative space created by the previous chapters and name the transparency tools that ought fill it. The law then delegates the creation of those tools to the ANPD, creating flexibility that allows for variance. In the best case, the ANPD establishes itself as a stalwart, and efficient defender of a right to data protection, setting and enforcing clear standards, and crucially using its role to update those standards keeping pace with changing technologies and markets. That flexibility also brings on meaningful risk, as the same powers could be used in the worst case to set weak standards, or even refuse to release them, making the law meek or even unenforceable.

Unfortunately the current composition of the ANPD, as described in chapter 9, does little to direct the agency towards that best case. By introducing a distinctly political character to the body, the law places Data Protection in the purview of the Brazilian executive, meaning what was described as a right is more likely to be treated as a lever of power. Under this paradigm presidents have the ability to change the extent to which Data Protection is enforced, leaving the right subject to the whims of particular administrations, and particularly vulnerable to lobbying by powerful data holding firms.

Some worrying signs can already be seen to be playing out since the law was passed. Following some changes to accommodate vetoes from president Temer, the final text of the law was presented in December 2018, and set to come into effect in August of 2020.<sup>57</sup> In the intervening years, Jair Bolsonaro of the far right *Partido Liberal* (Liberal Party) was elected, breaking an 18 year streak of left and center left governments. Bolsonaro has been openly hostile to digital governance with a specific focus on countering laws on disinformation, but bleeding into other fields. His willingness to extend that view to the functioning of the ANPD was recently observed by journalists Julio Wiziack and Ricardo Della Coletta, writing on government response to a 'megaleak' of personal information that took place in early 2022, reporting that the ANPD was forced to ask for help from the Federal Police and the Cabinet for Institutional Security due to "budgetary restraints and a lack of structure".<sup>58</sup> They predict that the organization will fail to hold perpetrators accountable, as it has not yet published a structure for investigations, or a schedule

---

<sup>57</sup> De Paula, Felipe, and Vitor Rabelo Naegele. 2022. "Há Vício De Iniciativa Na Criação Da Autoridade Nacional De Proteção De Dados?". *JOTA Info*. <https://www.jota.info/tributos-e-empresas/regulacao/ha-vicio-de-iniciativa-na-criacao-da-autoridade-nacional-de-protecao-de-dados-26072018>.

<sup>58</sup> Wiziack, Julio, and Ricardo Della Coletta. 2022. "Megavazamentos Expõem Fragilidade De Agência De Proteção De Dados". *Folha De S.Paulo*. <https://www1.folha.uol.com.br/mercado/2021/02/megavazamentos-expoem-fragilidade-de-agencia-de-protecao-de-dados.shtml>. - Translation provided by author.

for sanctions; both of which are set to be delivered in mid-2022, two years after the organizations inception.<sup>59</sup>

The first years of implementation can be expected to be rocky, but that observers find that the organizations woes are currently being compounded by issues of budget and organization is damning given the executive is directly responsible for resources provided to the ANPD it its first two years. This situation underlines the LGPD's current status as a law that provides meaningful rights and systems on paper, but who's implementation remains an open question.

---

<sup>59</sup> *ibid*

## Conclusion

Coming back to this investigation's principal question "*to what extent is the right to Data Protection entrenched in Brazilian legislation?*", the analysis carried out here indicates the answer is best given in parts. From a values standpoint, the legal foundation for a right to Data Protection is well voiced in Brazilian law, relying on an array of rights and guarantees started in the MCI and continued into the LGPD. As was seen, transparency, self determination, privacy, and autonomy are present in these laws in much the same way McDermott observed them in the European case.

From a systemic standpoint, as observed in the LGPD, Brazilian Data Protection is best described as an ambitious variation on a well respected model. LGPD chapters 1-3 build a normative framework for applying Data Protection that fits the bill of what is called for by the literature, using established definitions, and giving direction to the right through a robust conception of consent. The ambition comes in how the law foresees the creation of procedural mechanisms described in chapters 6-8; departing from its European inspiration by handing these powers to a new regulatory body, the ANPD, rather than stating them statically. This approach allows for a system that is better suited to regulate a fast changing environment, but brings with it meaningful risks.

Those risks are best understood when considering Data Protection from a procedural standpoint, where analysis has shown the law to be at its weakest. The body charged with publishing guidelines, conducting investigations, and administering sanctions is set up as a political entity controlled by the executive. The budgetary dependence placed on the ANPD during its first 2 years, matched with the sustained hold the executive has over the bodies all powerful Directing Council means the the strength of Data Protection in Brasil will be shaped by the president who controls the body in at the time of implementation, with subsequent administrations empowered to alter it as they see fit. Given digital regulations place as a contentious topic in Brazilian political discourse, and the interests at play, this configuration puts the right to Data Protection at risk.

Given this paradigm, improvement to Brazil's Data Protection laws are best done through changes in the procedural layer. There are two directions this can take: either shrinking the responsibilities given to the ANPD bringing the system closer to the European model, or by depoliticizing the body which could be done in a number of ways. Removing powers from the ANPD is the more stable route, as it restricts the power of the executive to make changes through political appointment. Depoliticizing the ANPD would likely entail curtailing the executives ability to appoint directors, this could look like extending terms and restricting the power of removal such that the executive couldn't reshape the body in their image, or creating a new system for appointment, perhaps making use of the multi-sectoral National Council for Data Protection and Privacy, amongst many other possibilities. In either case, it would likely take a lot of political

capital to wrestle power away from the executive, and theorizing on potential reform could certainly fill the pages several other investigations.



The EUI Academic Rules and Regulations for the Doctoral and Master's Programmes (Article 9.13. Publication of Thesis) state that:

"In accordance with Convention Article 14 (1), theses approved by an Examining Board must be published. Theses can be published on paper or in electronic format with an external publisher or in the open access electronic EUI repository. In the latter case, the copyright remains with the author. If the author decides not to agree to publication of the thesis in the EUI repository but fails to publish it with an external publisher within four years after the defence or has no firm indication of proximate publication, the EUI will automatically acquire the right to publish thesis in the EUI repository. These conditions shall be accepted by the author of the thesis in a signed agreement."

The author can – at any time – request the withdrawal of the fulltext ('unpublish' the thesis) from Cadmus, or the extension of the embargo lift date. Such requests will be treated on a case-by-case basis.

Before obtaining the PhD/Masters diploma this form<sup>1</sup> must be printed, filled out, signed by the author and sent to the relevant departmental assistant

Author's name: .....  
 Address: .....  
 Email: .....  
 Title of thesis: .....  
 Department: .....  
 Date of thesis defence:.....

Select: Ph.D.      Masters

**Choose option A or B below:**

**A) Open Access**  I authorise that my Ph.D./Masters thesis will be immediately published in Open Access on Cadmus, the EUI Research Repository. I have read and accept the terms of the Cadmus licence agreement <https://www.eui.eu/Documents/Research/Library/PublishingAndOpenScience/CadmusLicenceAgreement.pdf><sup>2</sup>  
 I declare that I alone am responsible for informing Cadmus, the EUI Research Repository ([cadmus@eui.eu](mailto:cadmus@eui.eu)) if/when the thesis is published elsewhere, wholly or in part. I take full responsibility for any obligations undertaken towards other publishers of all or parts of this thesis.

**B) Embargoed Access**  I authorise that my PhD/Masters thesis will be published in Open Access with Cadmus, the EUI Research repository, four years after the defence date in the case where at that point it has not been published commercially. I have read and accept the terms of the Cadmus licence agreement <https://www.eui.eu/Documents/Research/Library/PublishingAndOpenScience/CadmusLicenceAgreement.pdf><sup>3</sup>  
 I declare that I alone am responsible for informing Cadmus, the EUI Research Repository ([cadmus@eui.eu](mailto:cadmus@eui.eu)) if/when the thesis is published elsewhere, wholly or in part. I take full responsibility for any obligations undertaken towards other publishers of all or parts of this thesis.

Signature: .....      Date: .....

<sup>1</sup> This form is downloadable from:  
<https://www.eui.eu/Research/Library/PublishingAndOpenScience/Cadmus-SubmitFullTextTheses>

<sup>2</sup> The complete text of the Licence Agreement is on the back of this form.

<sup>3</sup> The complete text of the Licence Agreement is on the back of this form.

## Non-Exclusive Licence Agreement

By agreeing with and accepting this licence, I (the author, co-author, nominated agent or copyright owner) grant to Cadmus, the digital institutional repository of the European University Institute (EUI), or to any other digital repository authorized for use by the EUI, the non-exclusive right to reproduce, render (as defined below), and/or distribute my submission, referred to as the 'Work', worldwide in electronic format and in any medium for the lifetime of the repository.

### Non-exclusive rights and Cadmus

- Rights granted to Cadmus through this agreement are entirely non-exclusive.
- I give the right to EUI staff to deposit the Work for me
- I understand that depositing the Work in the repository does not affect my rights to publish the Work elsewhere, either in present or future versions.
- I understand that the Work deposited in Cadmus will be accessible to a wide variety of people and institutions, including automated agents and search engines via the Web.
- I understand that once the Work is deposited, metadata describing the Work may be incorporated into public access catalogues.
- Cadmus will clearly identify your name(s) as the author(s) of the Work, and will not make any alteration, other than as allowed by this licence, to your submission.
- Cadmus will respect any restrictions imposed by the copyright holders and/or publishing rights holders of the work as communicated by the author

### I. Agreement

I agree that:

1. Cadmus may, without changing the content, render the submission into any medium or format for the purpose of preservation.
2. Cadmus may keep more than one copy of this submission for purposes of security, back-up and preservation.
3. The EUI does not hold any obligation to take legal action on behalf of the depositor in the event of a breach of intellectual property rights or any other rights, in the Work.
4. The EUI does not hold any obligation to take legal action against a third party in the event of a breach of intellectual property rights or any other rights, in the use of the Work
5. Cadmus will file this Distribution Licence

### II. Declaration

I declare that:

1. I am the (co-)author or am acting on behalf of and have the authority of the (co-)author/s to make this agreement and do hereby give the EUI the right to make the Work available in the way described above.
2. the submission is the original work of the named (co-)author(s) and that I have the right to grant the rights contained in this licence
3. the submission is a true and accurate version of the published Work as permitted for deposit by the copyright holder and/or the holder of publishing rights of the Work; and that the moral rights of any co-authors of the Work have been respected
4. my submission does not, to the best of my knowledge, infringe upon copyright of third parties and does not breach any laws including those relating to defamation, libel, copyright or any other intellectual property rights.
5. if the submission contains third-party owned material (eg. data, images, extended quotations) for which I do not hold copyright, I have obtained the unrestricted and explicit permission of the copyright owner to grant Cadmus the rights required by this licence, and that such third-party owned material is clearly identified and acknowledged within the text or content of the submission.
6. If the submission is based upon work that has been sponsored or supported by an agency or organization, I have fulfilled any right of review or other obligations required by such contract or agreement.
7. That if, as a result of my having knowingly or recklessly given a false statement at points II.1-6 above, the EUI suffers loss, I will make good that loss and hereby indemnify the EUI for all action, suits, proceedings, claims, demands and costs occasioned by the University in consequence of my false statement.