INTERNATIONAL JOURNAL OF **DIGITAL AND DATA LAW**

REVUE INTERNATIONALE DE DROIT **DES DONNÉES ET DU NUMÉRIQUE**

Vol. 7 - 2021

ISSN 2553-6893

IMODEV
LES ÉDITIONS

International Journal of Digital and Data Law
Revue internationale de droit des données et du numérique

Direction :
Irène Bouhadana & William Gilles

ISSN : 2553-6893

IMODEV
49 rue Brancion 75015 Paris – France
www.imodev.org
ojs.imodev.org

Les propos publiés dans cet article n'engagent que leur auteur.

The statements published in this article are the sole responsibility of the author.

À PROPOS DE NOUS

La **Revue Internationale de droit des données et du numérique (RIDDN)/ the International Journal of Digital and Data Law** est une revue universitaire créée et dirigée par Irène Bouhadana et William Gilles au sein de l'IMODEV, l'Institut du Monde et du Développement pour la Bonne Gouvernance publique.

Irène Bouhadana, docteur en droit, est maître de conférences en droit du numérique et droit des gouvernements ouverts à l'Université Paris 1 Panthéon-Sorbonne où elle dirige le master Droit des données, des administrations numériques et des gouvernements ouverts au sein de l'École de droit de la Sorbonne. Elle est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Elle est aussi fondatrice et Secrétaire générale de l'IMODEV. Enfin, associée de BeRecht Avocats, elle est avocate au barreau de Paris et médiateure professionnelle agréée par le CNMA.

William Gilles, docteur en droit, est maître de conférences (HDR) en droit du numérique et en droit des gouvernements ouverts, habilité à diriger les recherches, à l'Université Paris 1 Panthéon-Sorbonne où il dirige le master Droit des données, des administrations numériques et des gouvernements ouverts. Il est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Il est aussi fondateur et Président de l'IMODEV. Fondateur et associé de BeRecht Avocats, il est avocat au barreau de Paris et médiateur professionnel agréé par le CNMA.

IMODEV est une organisation scientifique internationale, indépendante et à but non lucratif créée en 2009 qui agit pour la promotion de la bonne gouvernance publique dans le cadre de la société de l'information et du numérique. Ce réseau rassemble des experts et des chercheurs du monde entier qui par leurs travaux et leurs actions contribuent à une meilleure connaissance et appréhension de la société numérique au niveau local, national ou international en en analysant d'une part, les actions des pouvoirs publics dans le cadre de la régulation de la société des données et de l'économie numérique et d'autre part, les modalités de mise en œuvre des politiques publiques numériques au sein des administrations publiques et des gouvernements ouverts.

IMODEV organise régulièrement des colloques sur ces thématiques, et notamment chaque année en novembre les *Journées universitaires sur les enjeux des gouvernements ouverts et du numérique / Academic days on open government and digital issues*, dont les sessions sont publiées en ligne [ISSN : 2553-6931].

IMODEV publie deux revues disponibles en open source (ojs.imodev.org) afin de promouvoir une science ouverte sous licence Creative commons_CC-**BY-NC-ND** :

1) la *Revue Internationale des Gouvernements ouverts (RIGO)/ International Journal of Open Governments* [ISSN 2553-6869] ;

2) la *Revue internationale de droit des données et du numérique (RIDDN)/International Journal of Digital and Data Law* [ISSN 2553-6893].

ABOUT US

The **International Journal of Digital and Data Law / Revue Internationale de droit des données et du numérique (RIDDN)** is an academic journal created and edited by Irène Bouhadana and William Gilles at IMODEV, the Institut du monde et du développement pour la bonne gouvernance publique.

Irène Bouhadana, PhD in Law, is an Associate professor in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where she is the director of the master's degree in data law, digital administrations, and open governments at the Sorbonne Law School. She is a member of the Institut de recherche juridique de la Sorbonne (IRJS). She is also the founder and Secretary General of IMODEV. Partner at BeRecht Avocats, she is an attorney at law at the Paris Bar and a professional mediator accredited by the CNMA.

William Gilles, PhD in Law, is an Associate professor (HDR) in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where he is the director of the master's degree in data law, digital administration and open government. He is a member of the Institut de recherche juridique de la Sorbonne (IRJS). He is also founder and President of IMODEV. Founder and partner at BeRecht Avocats, he is an attorney at law at the Paris Bar and a professional mediator accredited by the CNMA.

IMODEV is an international, independent, non-profit scientific organization created in 2009 that promotes good public governance in the context of the information and digital society. This network brings together experts and researchers from around the world who, through their work and actions, contribute to a better knowledge and understanding of the digital society at the local, national or international level by analyzing, on the one hand, the actions of public authorities in the context of the regulation of the data society and the digital economy and, on the other hand, the ways in which digital public policies are implemented within public administrations and open governments.

IMODEV regularly organizes conferences and symposiums on these topics, and in particular every year in November the Academic days on open government and digital issues, whose sessions are published online [ISSN: 2553-6931].

IMODEV publishes two academic journals available in open source at ojs.imodev.org to promote open science under the Creative commons license CC-**BY-NC-ND**:

1) the *International Journal of Open Governments*/ la *Revue Internationale des Gouvernements ouverts (RIGO)* [ISSN 2553-6869] ;

2) the *International Journal of Digital and Data Law* / la *Revue internationale de droit des données et du numérique* (RIDDN) [ISSN 2553-6893].

COMPUTATIONAL PROPAGANDA AND DATA PROTECTION IN BRAZIL

by **João Victor ARCHEGAS**, Researcher at the Institute for Technology and Society of Rio de Janeiro, Brazil
and **Priscilla Silva LATERÇA**, Researcher at the Institute for Technology and Society of Rio de Janeiro, Brazil

In the beginning of 2015, the *Journal of Democracy* published a series of studies on democratic decline, including two papers by leading political scientists that reached competing conclusions about the overall health of democracy around the world. Larry Diamond famously argued that there was a democratic recession underway[1]. After decades of democratic ascension and consolidation, the rate of democratic failure was again on the rise, reaching a peak of 13% between 2004 and 2013[2]. Steven Levitsky and Lucan Way, on the other hand, called democratic recession a myth[3]. In their view, the evidence of backsliding was rather scarce and, therefore, the scholarly consensus that democracy is in deep trouble was nothing but an illusion. To them, the prevailing story is not one of recession, but instead of democratic resilience[4].

Fast forward to November of 2016 when Donald J. Trump was elected president of the US, forcing Americans to confront the fragility of their own democratic institutions and challenging the long-held belief of "American exceptionalism"[5]. It is hard to tell whether Levitsky still believes that democratic recession is a myth[6], but it is definitely telling that just a couple of years later he and his coauthor Daniel Ziblatt published the global bestseller *How Democracies Die*[7]. In their book, Levitsky and Ziblatt offer a compelling description of democratic backsliding across space and time. The book can be read as a cautionary tale or even an *exposé* of the illiberal rulebook. Nevertheless, the parallels between past and present are what made the book so bone-chilling when it was first published. Readers in countries that experienced democratic breakdown before were left with a disquieting feeling of *déjà vu*.

[1] L. DIAMOND, "Facing Up to the Democratic Recession", *Journal of Democracy*, Vol. 26(1), 2015.
[2] *Ibid*., p. 144.
[3] S. LEVITSKY and L. WAY, « The Myth of Democratic Recession », *Journal of Democracy*, Vol. 26(1), 2015.
[4] *Ibid*., p. 55-57.
[5] *See* C.R. SUNSTEIN (ed.), *Can It Happen Here? Authoritarianism in America*, Dey St., 2018.
[6] To be sure, it is possible to be concerned about the future of democracy and still hold on to the position that there was no democratic recession between 2004 and 2013.
[7] S. LEVITSKY and D. ZIBLATT, *How Democracies Die*, Crown, 2018.

At the same time, there was something new about how autocrats were undermining the predicates of democracy. Democracies were no longer not dying the old-fashioned way. There were no tanks on the streets, no *coup d'état*, no clear break from the preceding liberal regime. Instead, there was a slow and incremental dismemberment of the predicates of democracy. Nancy Bermeo accurately labeled this phenomenon a change in pace. In her words, "Troubled democracies are now more likely to erode rather than to shatter"[8]. Instead of a full-blown breakdown, the period of recession described by Diamond is characterized by democratic erosion, an "incremental, but ultimately still substantial, decay in the three basic predicates of democracy - competitive elections, liberal rights to speech and association, and the rule of law"[9].

Democratic erosion can be achieved through an array of different means. The autocrat can smear the reputation of journalists and leaders of the opposition to later dismiss any accusation of wrongdoing as "fake news". The constitutional system of checks and balances can become a preferred target, especially when watchdog institutions exercise their role and try to keep the autocrat at bay. In order to stay in power longer than it is legally permitted, the autocrat may try to leverage his popular support to amend the constitution and extend (or even extinguish) term limits. In other cases, when the autocrat's parliamentary support is strong enough, a new constitution can be adopted to cement a tilted electoral playing field. If evaluated in isolation, some of these changes may seem innocuous and even legitimate, but when stitched together they give rise to what Scheppele calls a "Frankenstate"[10]. Although the formal elements of a liberal and constitutional democracy may stay in place, its substance is significantly damaged (sometimes beyond repair)[11].

But there still is an underexplored side of the story. In our digital age, democratic erosion is technology-driven. Some authors acknowledge that disinformation campaigns on social media (or "fake news") are somehow connected to the decay of liberal democracies around the globe, but many stop short of making this discussion a core element of how they evaluate and offer solutions to the problems posed by democratic erosion. In other words, the

---

[8] N. BERMEO, "On Democratic Backsliding", *Journal of Democracy,* Vol. 27(1), 2016, p. 14.

[9] T. GINSBURG and A.Z. HUQ, *How to Save a Constitutional Democracy*, The University of Chicago Press, 2018, p. 43.

[10] K.L. SCHEPPELE, "The Rule of Law and the Frankenstate: Why governance checklists do not work", *Governance,* Vol. 26, 2013, p. 560 (in her words, the Frankenstate is "composed of perfectly reasonable pieces, and its monstrous quality comes from the horrible way that those pieces interact when stitched together").

[11] K.L. SCHEPPELE, *Worst Practices and the Transnational Legal Order (or How to Build a Constitutional "Democratorship" in Plain Sight)*, University of Toronto Faculty of Law Working Paper, 2016 [https://www.law.utoronto.ca/utfl_file/count/documents/events/wright-scheppele2016.pdf].

link between technology and democratic erosion is not just a footnote or a curiosity, but rather a central piece of the puzzle that will help us better understand and address this pressing challenge. In this paper, we use Brazil as a case study to assess how technology is being employed to hurt democracy – especially through the use of computational propaganda across social media platforms – and underscore the importance of data protection as a counteraction to this practice.

Throughout the paper, our objective is to show how democratic erosion and technology are intertwined in the digital age and, more specifically, how President Bolsonaro is using social media platforms to spread computational propaganda and entrench his political standing in Brazil. Furthermore, a key aspect of our argument is that data protection is a cornerstone of democracy in the digital realm. We will advance this position by looking at the *Cadastro Base do Cidadão* in Brazil, a centralized database created by Bolsonaro and designed to host a huge amount of personal data on Brazilian nationals. Our main concern is that, as it currently stands, the *Cadastro* violates some of the most basic principles and rules of the *Lei Geral de Proteção de Dados* or LGPD, Brazil's General Data Protection Law that was approved by Congress in 2018 and, after an unusually long period of *vacatio legis*, implemented in 2020.

In the next section, we discuss the relationship between social media platforms and democracy. Just like other new technologies, social networks can be used for good or bad purposes, enhancing or hurting democracy depending on the interests of particular political actors. In the third section, we offer a brief description of the state of computational propaganda in Brazil and how the *Cadastro* can be misused to advance ideological goals by the current or future presidents. In the fourth section, we elaborate on the features of the Brazilian General Data Protection Law and recount the story of how it came to fruition. In the fifth section, we argue that the *Cadastro* is inconsistent with some of the basic principles of the LGPD. Finally, in the sixth section, we offer some concluding remarks.

§ 1 – Social Media Platforms and Democracy

Florida is a battleground state in US presidential elections. In 2016, Trump won Florida's 29 electoral votes, beating Hillary Clinton and paving his way to the White House. Nevertheless, Clinton won in a few big counties, including a landslide victory in Miami-Dade where she received 63.2% of the vote. In 2020, polls conducted in the state favored Joe Biden by more than 2%. Even in the case of an upset, the Biden campaign was hoping to win big in Miami-Dade, repeating Clinton's results or even outperforming her. However, when the votes were tallied on election night, Trump won Florida by a 3.3% margin and Miami-Dade represented the most significant shift in the entire state. Biden still won in the county, but only received 53.4% of the vote, almost 10% less than

Clinton four years earlier. What exactly went wrong in Miami-Dade for the Biden campaign?

Political scientists are hard at work trying to understand what was behind this unexpected shift, but a couple of months before the election researchers were already worried about the effects of disinformation campaigns that targeted Latino immigrants in Miami. Ryan-Mosley, for example, noted that "the Trump campaign is feasting on genuine fears of communist rule and attempting to paint Biden as a socialist: A Trump ad campaign called '*Progressista*' compared some of Biden's language to that of Hugo Chavez, Fidel Castro, Gustavo Petro, and Nicolas Maduro, with a final screen that displays 'Biden = Socialism'". Furthermore, a big chunk of the disinformation was shared on WhatsApp groups. The messaging app is the preferred platform for immigrants because it "doesn't require a US phone number" and is particularly "hard to monitor and fact-check" due to end-to-end encryption, making it the perfect place to spread disinformation[12].

The electoral shift in Miami-Dade may be explained by what Helen Margetts calls the political turbulence generated by social media platforms. This new technology inaugurated the possibility for political mobilization to be structured around tiny political acts[13]. To put it differently, citizens can now participate in politics by donating small amounts of their time to a particular cause, which can be done by liking, sharing or commenting on a piece of content. There is no need to be affiliated with a political party or to attend a political gathering in order to be an active member of everyday public life. The cost of political participation plummeted with the emergence of social networks. On the other hand, this means that the traditional stabilizing elements of liberal democracies can now be bypassed on social media and that social scientists can no longer use traditional models to predict how (or if) these tiny political acts will scale up to become major political mobilizations.

The problem is that this phenomenon may lead to anti-democratic outcomes just as it can facilitate political participation in the digital age. In Margett's words, it can promote a "rise in political mobilisation and activism", but it can also foster "acts of misinformation, hate speech [...] and even terrorist influence"[14]. This is a key aspect of the relationship between social media and democracy. The same technology that can solve coordination

---

[12] T. RYAN-MOSLEY, « "It's been really, really bad": How Hispanic voters are being targeted by disinformation », *MIT Technology Review*, 2020 [https://www.technologyreview.com/2020/10/12/1010061/hispanic-voter-political-targeting-facebook-whatsapp/]. *See* also C. SESIN, « Did Trump draw out a new Latino Republican voter bloc in Florida? », *NBC News*, 2020 [https://www.nbcnews.com/news/latino/did-trump-draw-out-new-latino-republican-voter-bloc-florida-n1248577].

[13] H. MARGETTS, « Rethinking Democracy with Social Media », in A. GAMBLE and T. WRIGHT (eds.), *Political Quarterly Monograph Series*, 2019, pp. 107-23.

[14] *Ibid.*, p. 111.

hurdles and promote political movements like the Arab Spring can also be used as a tool to spread disinformation and undermine the predicates of democracy. What is more, the dynamic behind both possibilities is basically the same: tiny political acts scaling up in an unpredictable way. These tiny acts can also be understood as social information or information about what other people are doing or thinking.[15] On social media, social information is presented instantly through popularity indicators.[16]

In other words, users can know what other people are endorsing (or rejecting) just by taking a quick glance at these indicators (for example, how many likes, hearts or laughs a publication has on Facebook). With this social information on their hands, users can make their own decisions and choose whether to undertake particular tiny political acts or not (for example, adding a like, heart or laugh to that particular post). Over time (and on social media we may be talking about just a few hours or minutes), these tiny political acts can scale up to the point they become major mobilizations and effectively shape the political landscape. Social media, therefore, are not just about winning or losing elections. The political use of digital platforms may have an electoral impact – like in the above-mentioned Miami-Dade case –, but it cuts deeper than that. "Social media [...] are embedded in political life"[17]. What is more, it represents a new dimension of political life, one where tiny political acts and social information emerge as central pieces.

The way people respond to the advent of social media as political spaces has gone through a few stages that mimic, at least to some extent, the five stages of grief[18]. First, people deny that social media actually brings something new to the table and argue that it is just a new arena for doing politics. Second, people enter a stage of bargaining where the prevailing idea is that the internet should remain open and free so that the transformation of politics can reach its full beneficial potential. Third, people grow angrier and start to blame social media for the decline of democracy around the world. Fourth, depression hits and people start talking about impending doom and the emergence of a post-truth era. But now, after experiencing the first four stages, we may be finally ready to accept social media as part of our political life so we can "accommodate the change through a process of institutional catch-up".[19]

---

[15] Scott A. Hale *et al*, "How Digital Design Shapes Political Participation: A natural experiment with social information", *PLoS ONE Journal,* Vol. 13(4), 2018, p. 4.

[16] *Ibid*., p. 15.

[17] H. MARGETTS, "Political Behavior and the Acoustics of Social Media", *Nature Human Behavior*, Vol. 1(86), 2017, p. 2.

[18] H. MARGETTS, "Rethinking Democracy with Social Media", in A. GAMBLE and T. WRIGHT (eds.), *Political Quarterly Monograph Series*, 2019, pp. 113-15.

[19] *Ibid*., p. 115.

In the discussion that follows, we accept that social media is here to stay and that it can have good or bad consequences for democracy depending on how, by whom and for what purposes it is employed. It is only by accepting the political dimension of social media that we can move past existing gridlocks and think about solutions to the challenges we face. In the next section, we focus on a particular challenge posed by the political dimension of social networks: computational propaganda (CP). After defining the concept, we show how the Bolsonaro administration takes advantage of CP to advance its political interests in Brazil. Towards the end of the section, we argue that the recently created *Cadastro Base do Cidadão* may represent a risk to democracy in the country and that data protection is an important guardrail against its potential abuses. Or, to use the words above, data protection is one element of the "institutional catch-up" strategy that can help us advance democracy in the digital age.

§ 2 – COMPUTATIONAL PROPAGANDA, DATA PROTECTION AND THE *CADASTRO BASE DO CIDADÃO*

Computational propaganda (CP) can be defined as the employment of new technologies, namely big data analytics and automation, to channel public discourse in favor of a political ideology. In Bradshaw and Howard's words, it is "the use of algorithms, automation, and big data to shape public life"[20]. Propaganda is definitely not a new concept. According to the Merriam-Webster dictionary, the first known use of the term can be traced back to 1622, when Pope Gregory XV created the *congregatio de propaganda fide,* an organization of the Catholic Church responsible for the evangelization of non-Catholic communities with a focus on colonies in the Global South. The term was repurposed in the XX century to explain the manipulation of the public's perception of an enterprise (political or commercial) through the use of language (written, spoken, and visual)[21].

In the digital age, the goal of propaganda is basically the same (to change people's mind about something), but the means to achieve it have drastically changed. Governments and political parties now subsidize the work of cyber troops to spread CP across social networks. These troops are "publicly funded and often highly coordinated government actors who use social media to spread

[20] S. BRADSHAW and P.N. HOWARD, "The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation", *Working Paper – Oxford Computational Propaganda Research Project*, 2019, p. I, [https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2020/10/CyberTroop-Report19_V2NOV.pdf].

[21] *See*, for example, E. BERNAYS, *Propaganda*, Ig Publishing, 2004 (the original work was published in 1928 by Routledge, where Bernays famously wrote that "the conscious and intelligent manipulation of the organized habits and opinions of the masses is an important element of democratic society. Those who manipulate this unseen mechanism of society constitute an invisible government which is the true ruling power of our country").

disinformation and attempt to generate false consensus"[22]. The canonical example is the Russian troll factory or Internet Research Agency (IRA), the private organization with close ties to the Kremlin that meddled in the 2016 US presidential election in favor of Donald J. Trump[23]. Nevertheless, the Russian blueprint for online manipulation has now gone global. According to an international survey of cyber troop activity conducted annually by Bradshaw and Howard, the evidence of CP rose from 28 countries in 2017 to 70 countries in 2019, an increase of 150% in just two years[24]. Furthermore, the prevailing types of messages used in CP are "pro-government or pro-party" alongside "smear campaigns" aimed at the political opposition[25].

In Brazil, CP has been a hallmark of Bolsonaro's presidency. Before his election in 2018, Bolsonaro was just another low-key politician in Brasília where he spent almost three decades of his career in Congress as an elected representative from the state of Rio de Janeiro. He was part of what journalists call "the lower clergy of politics", a group of political outcasts that have no big ambitions other than being reelected every four years. But around 2014 and 2015 he became something he might have never anticipated: a social media celebrity. Videos of his inflammatory and repulsive remarks began to surface around the web in the form of "memes" calling him *mito* (myth in Portuguese). One of the early clips showed him arguing with leftist congresswomen Maria do Rosário and saying that he "would never rape her" because she "do not deserve it"[26]. Meme after meme, Bolsonaro rose to digital stardom and, to everyone's surprise, became a viable presidential candidate, presenting himself as someone who was not afraid to defy the "politically correct" and as a proud outcast while a "corrupt elite" ruled the country.

Without social media, it is unlikely that Bolsonaro would become anything more than a fringe politician. Evidence of this is that some memes went back a number of years to resurrect some of his most divisive remarks, including one from the late 90s when, during an interview, he called for the execution of former president Fernando

---

[22] S. BRADSHAW and P.N. HOWARD, "The Global Organization of Social Media Disinformation Campaigns", *Journal of International Affairs*, Vol. 71(1.5), 2018, p. 24.

[23] For an early investigation into the IRA, *see* A. CHEN, "The Agency", *The New York Times Magazine,* 2015 [https://www.nytimes.com/2015/06/07/magazine/the-agency.html].

[24] S. BRADSHAW and P.N. HOWARD, "The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation", *Working Paper – Oxford Computational Propaganda Research Project*, 2019, p. 2 [https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2020/10/CyberTroop-Report19_V2NOV.pdf].

[25] *Ibid.*, p. 13.

[26] A.J. KAISER, "Woman who Bolsonaro insulted: 'Our president-elect encourages rape'", *The Guardian*, 2018 [https://www.theguardian.com/world/2018/dec/23/maria-do-rosario-jair-bolsonaro-brazil-rape].

Henrique Cardoso and said that if he ever became president he would close Congress the very next day because "elections won't change anything in this country"[27]. At the time those remarks were originally made, legacy media did not echo Bolsonaro's words. But now, with the advent of many-to-many means of communication, things have changed. According to Urbinati, social media now offer a form of "horizontal simplification" of political mobilization[28]. As a result, the intermediary role of the independent press (and even of political parties) is significantly weakened by the emergence of "live streaming democracy" – or, to put it differently, traditional intermediaries can now be bypassed on digital platforms[29].

Nonetheless, Bolsonaro did not only take advantage of social media to bypass intermediaries and speak directly to his electorate, he also saw an opportunity to build a lie machine with the potential to outlast his electoral bid and become an essential tool for governing the country. As Howard explains, "a lie machine is a system of people and technologies that distribute false messages in the service of a political agenda"[30]. Or, to use different terms, it is the use of information technologies to produce, market, and distribute political lies in the form of CP[31]. During the 2018 election, Bolsonaro and his staffers turned the messaging service WhatsApp into the backbone of their political strategy[32]. They created countless groups on the platform and posted hyperlinks on public forums so people could easily join them. These groups were then used by the campaign as nodal points to spread propaganda in a coordinated (albeit decentralized) fashion[33].

As Arnaudo notes, Brazil had previous experiences of CP that endured longer than the timeframe of elections. An example is the smear campaign promoted by former presidential candidate Aécio Neves against former president Dilma Rousseff. Neves lost the 2014 runoff to Rousseff but he did not concede the race and repurposed his lie machine to push for Rousseff's impeachment (which was ultimately achieved in 2016)[34]. However, Bolsonaro is

---

[27] S. MEREDITH, "Who is the 'Trump of the Tropics'?: Brazil's divisive new president, Jair Bolsonaro – in his own words", *CNBC*, 2018 [https://www.cnbc.com/2018/10/29/brazil-election-jair-bolsonaros-most-controversial-quotes.html].

[28] N. URBINATI, "A Revolt against Intermediary Bodies", *Constellations*, Vol. 22, 2015, p. 478.

[29] *Ibid.*, 478-80.

[30] P.N. HOWARD, *Lie Machines: How to save democracy from troll armies, deceitful robots, junk news operations, and political operatives*, Yale University Press, 2020, p. 13.

[31] *Ibid.*, p. 16.

[32] P.C. MELLO, *A Máquina do Ódio: notas de uma repórter sobre fake news e violência digital*, Companhia das Letras, 2020, p. 22.

[33] *Ibid.*, pp. 31-33.

[34] D. ARNAUDO, "Brazil: Political Bot Intervention During Pivotal Events", in S. WOOLLEY and P.N. HOWARD (eds.), *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*, Oxford University Press, 2019, pp. 138 and 147.

the first *sitting* president to use CP as a core strategy of his administration. There are now two ongoing investigations, one in Congress and a second in the Supreme Federal Tribunal, looking into allegations that Bolsonaro, his sons, and a few close aides operate what journalists call "the office of hate", the Brazilian version of the Russian troll factory[35]. After all, like the Washington Post noted, "Virtually anyone who criticizes Bolsonaro […] draws overwhelming and coordinated digital smears"[36].

The fuel for a lie machine is data. To produce, market, and distribute computational propaganda across social networks, political actors need some amount of behavioral data on their targets. True, different cyber troops have different levels of formal organization[37] and this may impact the way (and to what extent) they use data to power up their activities. However, the shift from *polling* data to *behavioral* data still is one of the most significant in modern politics. As Howards notes, "Politicians used to have polling data and surveys to interpret what voters are thinking" and "now we have behavioral data about what people *actually* do"[38]. The source of our concern over online disinformation is not really the content that is being distributed, but instead the data we constantly share about ourselves that is then employed to make disinformation campaigns so effective[39]. As noted above, propaganda techniques can be traced back to, at the very least, 1622. What is new is that behavioral data is now available to political actors alongside the automated tools they have at their disposal to advance CP.

In his book on democratic decline, Diamond notes that "the greatest danger [to democracy] is industrial-scale truth distortion as governments and political groups launch highly organized information operations"[40]. Scholars disagree over the ideal counteractions to dismantle these operations, but it is clear that the flow of data is at the very heart of the problem. The biggest danger

---

[35] There are, however, a few differences between the Russian IRA and Bolsonaro's "office of hate". For starters, the office is composed of government officials with close ties to the president and his sons who are said to receive direct orders from them. On the other hand, the office and the IRA operate in very similar ways, patrolling the web, producing reports and ultimately promoting smear campaigns against opponents and glorifying the work of the ruling coalition.

[36] T. MCCOY, "An investigation into fake news targets Brazil's Bolsonaros, and critics fear a constitutional crisis", *The Washington Post*, 2020, [https://www.washingtonpost.com/world/the_americas/brazil-bolsonaro-fake-news-coronavirus/2020/06/03/60194428-a4de-11ea-898e-b21b9a83f792_story.html].

[37] S. BRADSHAW and P.N. HOWARD, "The Global Organization of Social Media Disinformation Campaigns", *Journal of International Affairs,* Vol. 71(1.5), 2018, p. 27.

[38] P.N. HOWARD, *Lie Machines: How to save democracy from troll armies, deceitful robots, junk news operations, and political operatives*, Yale University Press, 2020, p. 3.

[39] *Ibid*., 10.

[40] L. DIAMOND, *Ill Winds: Saving democracy from Russian rage, Chinese ambition, and American complacency*, Penguin Press, 2019, p. 232.

to democracy is not false information *per se*, but the concentration of behavioral data in a few hands, which enables the spread of disinformation at an industrial-scale. Or, as Howard argues, we should not be looking too closely at distorted content, which is just a symptom of the problem we face, but instead we should focus on "repairing the flow of data within democracies"[41]. Therefore, it is urgent that we think about data protection as one of the main counter strategies to curb the spread of CP throughout the digital sphere.

This is why the creation of the *Cadastro Base do Cidadão* in Brazil is so troubling. Data grabs by national governments are the latest in a series of actions that drive democratic erosion and help concentrate political power in detriment of democratic accountability. In October of 2019, Bolsonaro signed a decree creating a new data-sharing system within the national government to make a centralized database on Brazilians' personal data viable. Now, all the eggs are in the same basket. What is more, the decree allows government bodies to request data from other government bodies without citizens ever knowing about it. It took leaked documents and a journalistic investigation for Brazilians to learn that the Brazilian Intelligence Agency requested data on all drivers in the country, including the pictures on driver's licenses.[42]

More concerning still, Bolsonaro's decree creates a new Central Data Governance Committee that will have oversight of the data hosted by the *Cadastro*. The committee will be composed exclusively of federal government actors appointed by the president, without the involvement of other stakeholders (academics, civil society organizations, citizens, and so on). Therefore, Bolsonaro's plan is not just an all-the-eggs-in-the-same-basket approach, it is a placing-the-fox-to-guard-the-henhouse approach, where all the eggs wait to be picked off. With this institutional design in place, Bolsonaro has complete control over the *Cadastro*. This weakens the government's argument that a centralized database would enhance public services and raises concerns that the data will be used to politically profile citizens and fuel Bolsonaro's lie machine.[43] These concerns are far from being unsubstantiated given that recent leaked documents show that the Bolsonaro administration is already collecting data on the behavior of journalists and "political detractors" on social media.[44] In the

---

[41] P.N. HOWARD, *Lie Machines: How to save democracy from troll armies, deceitful robots, junk news operations, and political operatives*, Yale University Press, 2020, p. 162.

[42] T. DIAS and R.M. MARTINS, "Documentos vazados mostram que ABIN pediu ao SERPRO dados e fotos de todas as CNHS do país", *The Intercept Brasil*, 2020 [https://theintercept.com/2020/06/06/abin-carteira-motorista-serpro-vigilancia/].

[43] R. KEMENY, "Brazil is sliding into techno-authoritarianism", *MIT Technology Review*, 2020, [https://www.technologyreview.com/2020/08/19/1007094/brazil-bolsonaro-data-privacy-cadastro-base/].

[44] R. VALENTE, "Relatório do governo separa em grupos jornalistas e influenciadores", UOL Notícias, 2020

next two sections, we go over the story of Internet governance and data protection in Brazil to show how the *Cadastro* violates Brazil's General Data Protection Law.

§ 3 – BRAZIL'S FRAMEWORK FOR INTERNET GOVERNANCE AND DATA PROTECTION

Over the past fifteen years or so, Brazil earned a place as a global reference on the promotion of multi-stakeholder, collaborative legislative processes and public policy-making in the field of Internet governance. Since the creation of the Brazilian Internet Steering Committee (CGI.br)[45] in the 90s, Brazil implemented a number of principles for Internet governance – based on multilateral, transparent and democratic practices – and selected representatives from civil society to participate in discussion rounds to debate priorities for the Internet alongside government officials. It was exactly the consolidation of this innovative model of Internet governance that encouraged an increase in the technical quality of digital services in the country, and, of course, their dissemination across Brazil.

In the first decades of the XXI century, Brazil further consolidated its status as a beacon of Internet governance with the promulgation of the Internet Bill of Rights (*Marco Civil da Internet* in Portuguese)[46]. The legislative discussion was prompted by the Edward Sowden scandal, which revealed how the American NSA was monitoring the communications of other countries without their consent, including Brazil. Presenting itself as an affirmative statement of values and rights, which aims to translate fundamental principles of the 1998 Constitution to the digital realm – such as net neutrality, freedom of expression, and data protection –, the Internet Bill of Rights established state-of-the-art mechanisms to promote digital identity authentication and intermediary liability rules for illegal content hosted on digital platforms[47].

Discussions and negotiations on the new law took place over many years and consisted of multiple, complex phases. Ultimately, the success of the project can be attributed to the multi-stakeholder process that guided all the discussions in Congress. What is more, the process was marked by a forceful public reaction against the passing of a cybercrime bill in Brazil, which would have limited some fundamental liberties on the cyber sphere had it been passed

[https://noticias.uol.com.br/colunas/rubens-valente/2020/12/01/governo-bolsonaro-jornalistas-redes-sociais.htm].

[45] *See* more about CGI at [https://www.cgi.br/about/].

[46] *See* an English Translation of the Internet Bill of Rights at: [https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180].

[47] For a discussion on how the Internet Bill of Rights is connected to the idea of "digital constitutionalism", *see* L.F.M. MONCAU and D.W. ARGUELHES, "The Marco Civil da Internet and Digital Constitutionalism", in G. FROSIO, *Oxford Handbook of Online Intermediary Liability*, 2020.

into law (providing a blueprint for discussions over SOPA and PIPA in the United States years later)[48] [49].

The final text of Brazil's Internet Bill of Rights attracted broad international support, from the father of the World Wide Web, Sir Tim Berners-Lee[50], to the rapporteurs for freedom of expression of the United Nations (UN)[51] and the Organization of American States (OAS)[52]. The Brazilian law also served as an inspiration for other documents that were adopted around the globe in the following years, including the crowdsourced Declaration of Internet Rights approved by the Italian Parliament in 2018.

Four years after the adoption of the Internet Bill of Rights, Brazil's Congress approved a general data protection law (*Lei Geral de Proteção de Dados* - LGPD),[53] closely modeled after the European General Data Protection Regulation (GDPR). Just like the Internet Bill of Rights, discussions over the Brazilian Data Protection Law were marked by collaborative processes during which input and feedback from all stakeholders were taken into account in an equitable and horizontal manner. The drafting of the new law also took Human Rights principles in consideration and used the Universal Declaration of Human Rights as a basis for the discussion rounds.

Nevertheless, even before the LGPD was passed into law by the National Congress in 2018, courts in Brazil were already developing data protection mechanisms through case-by-case analysis. To do that, judges relied on the right to privacy under the 1988 Constitution and other key provisions of the 2002 Civil Code. The 1990 Consumer Protection Code and the 2014 Internet Bill of Rights also have provisions that precede the LGPD and are, to some extent, dedicated to data protection. However, just like the GDPR in Europe, the new Brazilian Data Protection Law is the first of its kind; a legal document entirely dedicated to the protection of personal data with provisions that bind both the public and private sectors.

---

[48] C.A. SOUZA, M. VIOLA and R. LEMOS (eds.), *Brazil's Internet Bill of Rights: A Closer Look.*, Second Edition, 2017, p. 41 [https://itsrio.org/wp-content/uploads/2018/02/v5_com-capa__pages_miolo_Brazil-Internet-Bill-of-Rights-A-closer-Look.pdf].

[49] *See* more on the protests against SOPA and PIPA at: [https://en.wikipedia.org/wiki/Protests_against_SOPA_and_PIPA]

[50] World Wide Web Foundation, *Welcoming Brazil's Marco Civil: A World First Digital Bill of Rights*, 2014 [https://webfoundation.org/2014/03/welcoming-brazils-marco-civil-a-world-first-digital-bill-of-rights/].

[51] F. LARUE *et al*, *Joint Declaration on Freedom of Expression and the Internet*, Inter-American Commission on Human Rights, 2011 [http://www.oas.org/en/iachr/expression/showarticle.asp?artID=849&lID=1].

[52] E. LANZA, « Standards for a Free, Open and Inclusive Internet », OAS, 2017 [http://www.oas.org/en/iachr/expression/docs/publications/INTERNET_2016_ENG.pdf].

[53] *See* an English Version of Brazil's General Data Protection Law at [https://www.mattosfilho.com.br/EscritorioMidia/MattosFilho_brazilian_data-protection-law.pdf].

Despite the extensive democratic debate and all the legal initiatives that strove to consolidate a culture of data protection in Brazil, the approval and implementation of the law was nowhere near the straightforward procedure many had hoped for, chiefly because the federal government maneuvered to delay the enactment of the new law[54]. A few weeks before the approval of the LGPD in Congress, while the project was still under discussion in a few House committees, media outlets reported that the government was attempting to modify the text that would then be sent to a final vote on the Congress floor. The national government's main objective was to remove from the document several obligations that, if the project was approved, would fall on the public sector.

Fortunately, the attempt proved to be unsuccessful and the LGPD ended up consolidating the idea that the public sector is one of the main "data controllers" in the country and, in light of the digitalization process the government is going through, it is paramount for the effective implementation of a data protection framework that the Brazilian state is constrained by the provisions of the new law, respecting, among others, the obligation to invest in security protocols, an area that was neglected by the government before and that received more attention during the COVID-19 public emergency[55] [56].

Nevertheless, even after the approval of the LGPD with all the provisions concerning the public sector in place, some rules were

---

[54] A. ROSSO, *LGPD e setor público: aspectos gerais e desafios* [https://www.migalhas.com.br/depeso/300585/lgpd-e-setor-publico--aspectos-gerais-e-desafios]

[55] Just like other countries, Brazil used geolocation data to monitor the evolution of the pandemic. However, this sparked fears of possible privacy breaches, as the general data protection law was not yet in force and the national government has a history of data leaks. *See* M. SCHREIBER, "Coronavírus: uso de dados de geolocalização contra a pandemia põe em risco sua Privacidade?", *BBC News Brazil*, 2020, [https://www.bbc.com/portuguese/brasil-52357879]; and C. CIMPANU, "Personal data of 16 million Brazilian COVID-19 patients exposed online", *ZDNet*, 2020, [https://www.zdnet.com/article/personal-data-of-16-million-brazilian-covid-19-patients-exposed-online/].

[56] The Brazilian government has been treating data in an authoritarian fashion and the pandemic aggravated this situation. In April of 2020, the president signed a decree, mandating that telecom companies hand over data on 226 million Brazilian citizens to the Brazilian Institute of Geography and Statistics under the pretext of monitoring income and employment levels during the pandemic. According to the decree, telecom companies should hand over lists of names, phone numbers and addresses of their consumers for the research to fight the COVID pandemic. In May, the Brazilian Supreme Federal Court established that this was incompatible with basic principles of privacy and data protection. But what shines through the case is the lack of clarification around data security mechanisms by the presidential decree. The arguments advanced by the Supreme Court include: (i) Lack of clear definitions and purpose; (ii) Violation of constitutional principles; (iii) Lack of fundamental safeguards; (iv) Lack of necessity and proportionality; (v) Lack of technical mechanisms to prevent accidental leaks. *See* the decision in Portuguese at [http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=442902].

vetoed by President Bolsonaro. Among others, the most eye-catching are the ones that referred to the creation of the National Data Protection Authority (*Autoridade Nacional de Proteção de Dados* – ANPD). Bolsonaro's veto and subsequent attempts to delay the application of the law made academics and political actors fearful that the LGPD would become ineffective (or even meaningless) even before it came into full force. After all, the president was fighting hard to shield the federal government from the new data protection framework and to co-opt the National Authority.

After the back-and-forth between the president and congress, several textual modifications, and, finally, the creation of a new National Data Protection Authority through a presidential provisional measure[57], the LGPD entered into force on September 18, 2020. Yet, its enforcement provisions (including several administrative penalties) will not be implemented until August of 2021. Another significant challenge is that the creation of a new National Authority through a presidential provisional measure came at a high cost: The ANPD was established under the direct supervision of the Presidential Office, which, again, raises suspicions about its independence vis-à-vis the federal government and its ability to make decisions that, albeit necessary from a data protection standpoint, may displease the public sector.

In sum, the story of the LGPD in Brazil unfolded in two distinct (and at times conflicting) acts. First, the initial draft underwent a democratic and participatory process in Congress, resulting in an innovative legal document that promised an effective and dynamic data protection framework for the country. Second, after the election of Bolsonaro in 2018 (the same year that the LGPD was approved in Congress), Brazil veered down a more authoritarian path. Bolsonaro took issue with some of the law's provisions (namely those that imposed obligations to the Public Sector) and brought the ANPD under his sphere of influence. What is more, under Bolsonaro, the implementation of facial recognition technologies and massive and disproportionate data grabs by the national government became a reality. All that was happening while the LGPD and the National Authority were still receiving some final touches[58]. It was like Bolsonaro perceived the new law as an obstacle to his political ambitions, so he used all the tools at his disposal to nuke the pillars of the recently created data protection framework, making sure it would not stand in his way.

---

[57] Provisional Measure No. 869 of 2018, amending Law No. 13.709/2018 to provide for the protection of personal data and create the National Data Protection Authority. *See* the text in Portuguese at: [https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/135062]

[58] Coalizão Direitos na Rede, *Open Letter from the Brazilian Civil Society on the occasion of the 15th edition of the United Nations Internet Governance Forum*, 2020, [https://direitosnarede.org.br/2020/11/17/open-letter-from-brazilian-civil-society-on-the-occasion-of-the-15th-edition-of-the-united-nations-internet-governance-forum/].

It was in this context that, in October of 2019, President Jair Bolsonaro signed a decree – without any previous debate or public consultation – to simplify the data-sharing system between different federals bodies and agencies and compelling them to share most of the data they hold on Brazilian citizens, from health records to biometric information, in favor one vast and centralized database known as the Citizens' Basic Register (*Cadastro Base do Cidadão*). The database will be operated by the Secretary of Digital Government under the auspices of the Ministry of Economy and, depending on the category of data in question, other ministries and public authorities in general will be able to access tons of personal information with little to no restriction. Initiatives such as the Citizens' Basic Register open up the possibility for the government to misuse its data-collection prerogative and represent a threat to the achievements of the General Data Protection Law, as we shall see below.

§ 4 –THE RISKS INVOLVED IN THE IMPLEMENTATION OF THE *CADASTRO*

By establishing a new data-sharing system and terminating the need for formal agreements or contracts when data is requested for "research purposes" – which is a very broad idea that can be used as a catch-all concept –, the decree leaves room for vast government surveillance of the population and for unchecked data flows within the national government, without ever mentioning the requirements of the LGPD that should restraint the collection and treatment of personal data. This can give place to an intricate situation because it forces sensitive decisions to be made in a case-by-case basis when a general data protection framework is already available. Under the pretext of fostering innovation and enhancing public services, the decree may allow unwarranted access to a very rich and extensive data set. It is an unprecedented instance of unification and centralization of personal data.

The concentration of sensitive data in a single database – such as genetic materials, faces, and even fingerprints – as a form of identifying people, without them knowing exactly how, represents a violation of the principle of transparency and makes it harder to monitor compliance with the principle of non-discrimination, two cornerstones of the LGPD. In a society marked by profound inequalities that are inevitably reflected in the personal data collected by the government, the management of information and its use for decision-making must be placed under intense scrutiny, criticism and control. It is worth remembering that in the Brazilian context, episodes of predictive policing that disproportionately impact political minorities and the unequal access to "intelligent health" by the black population have been increasingly frequent.

It is also worth noting that across-the-board surveillance techniques bring back memories of a violent and repressive chapter of Brazilian history. On the one hand, the country remained under

an undemocratic and authoritarian military regime from 1964 – when a military coup ousted President João Goulart – until 1985 – when a transition to democracy finally gained traction with the election of a non-military president. On the other hand, the current Bolsonaro administration, to some extent, represents a comeback of the military to the federal government. Bolsonaro himself is a former army captain and he appointed countless military personnel to key government positions. The inconsistencies between the *Cadastro Base do Cidadão* and the Brazilian Data Protection Legislation, in light of recent Brazilian history, poses a serious risk to democracy.

The rampant militarization of the national government is illustrated by a recent case revealed by The Intercept in June of 2020 that was briefly mentioned above. The Brazilian National Intelligence Agency (ABIN) used the new decree to ask Serpro, a state-owned technology company, for the records of 76 million Brazilian citizens who hold driver's licenses[59]. This example illustrates how data could start appearing in many new data sets without data subjects ever knowing about it, moving the country towards an unbridled surveillance state in detriment of the public interest – something that can only reinforce existing asymmetries between data subjects and the state.

The unified database also raises concerns about security breaches. The decree addresses security as an imprecise obligation, one that will be further interpreted by managers and the Central Data Governance Committee. The Committee, as noted above, lacks institutional independence and will be composed solely of government actors, raising concerns over its ability to protect citizens' personal data from the government itself. Data security is a constituent element of the right to privacy and informational self-determination. A centralized database and a data-sharing system that do not have data security as a priority should be treated with caution and suspicion. Once again, the inconsistency between the Cadastro and the LGPD is patent[60].

All these inconsistencies, when evaluated in conjunction, show that Bolsonaro's decree violates the most basic principles and rules of the LGPD and, because of that, the *Cadastro* is vulnerable to be misused as a source of behavioral and personal data in the

[59] T. DIAS and R.M. MARTINS, "Documentos vazados mostram que ABIN pediu ao SERPRO dados e fotos de todas as CNHS do país", *The Intercept Brasil*, 2020, [https://theintercept.com/2020/06/06/abin-carteira-motorista-serpro-vigilancia/].

[60] Due to recent data leaks, the level of concern around possible breaches is high. In December 2020, for example, Brazil experienced a major leak of public health data under the Ministry of Health's watch. *See* A. HOPE, "Brazil's Health Ministry's Website Data Leak Exposed 243 Million Medical Records for More Than 6 Months", *CPO Magazine*, 2020, [https://www.cpomagazine.com/cyber-security/brazils-health-ministrys-website-data-leak-exposed-243-million-medical-records-for-more-than-6-months/].

production and distribution of computational propaganda[61]. In this sense, the Citizen's Basic Register, as it currently stands, could be used as an instrument for advanced profiling, including through the treatment of data gathered during the pandemic, and to identify voters that are most likely to believe in and spread misleading information. All in all, the combination of the lack of security over the *Cadastro* with the concerning trend of democratic backsliding in Brazil point to the reinforcement of Bolsonaro's hate/lie machine[62].

CONCLUSION

Computational propaganda is driving democratic erosion in the digital age. There is much to be said about this troubling (yet far from trivial) connection. In this paper, we aimed to tackle a fraction of the problem and show how the *Cadastro Base do Cidadão* in Brazil, as it currently stands, can be misused as an easily-accessible source of behavioral data to power up Bolsonaro's lie machine. We argued that data protection is a key element of the "institutional catch-up" game we need to play in order to curb the spread of coordinated disinformation campaigns that deeply hurt liberal democracies. Going forward, it is essential that scholars think about how to restructure the flow of data within democracies to prevent its concentration in the hands of illiberal leaders.

BIBLIOGRAPHY

ARNAUDO D., "Brazil: Political Bot Intervention During Pivotal Events", in S. WOOLLEY and P.N. HOWARD (eds.), *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*, Oxford University Press, 2019

BERMEO N., "On Democratic Backsliding", *Journal of Democracy,* Vol. 27(1), 2016

BRADSHAW S., P.N. HOWARD, "The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation", *Working Paper – Oxford Computational Propaganda 29. Research Project*, 2019.
[https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2020/10/CyberTroop-Report19_V2NOV.pdf]

[61] R. KEMENY, "Brazil is sliding into techno-authoritarianism", *MIT Technology Review*, 2020
[https://www.technologyreview.com/2020/08/19/1007094/brazil-bolsonaro-data-privacy-cadastro-base/].

[62] C. TARDÁGUILA, *How techno-populists put the 'Hate Machine' to work in spreading disinformation*, Poynter, 2020,
[https://www.poynter.org/fact-checking/2020/how-techno-populists-put-the-hate-machine-to-work-in-spreading-disinformation/].

BRADSHAW S., P.N. HOWARD, "The Global Organization of Social Media Disinformation Campaigns", *Journal of International Affairs,* Vol. 71(1.5), 2018

Brazil's General Data Protection Law (English translation) [https://www.mattosfilho.com.br/EscritorioMidia/MattosFilho_brazilian_data-protection-law.pdf]

Brazil's Internet Bill of Rights (*English translation*) [https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180]

CHEN A., "The Agency", *The New York Times Magazine*, 2015 [https://www.nytimes.com/2015/06/07/magazine/the-agency.html]

CIMPANU C., "Personal data of 16 million Brazilian COVID-19 patients exposed online", *ZDNet*, 2020, [https://www.zdnet.com/article/personal-data-of-16-million-brazilian-covid-19-patients-exposed-online/]

CNBC, 2018 [https://www.cnbc.com/2018/10/29/brazil-election-jair-bolsonaros-most-controversial-quotes.html]

COALIZÃO DIREITOS NA REDE, *Open Letter from the Brazilian Civil Society on the occasion of the 15th edition of the United Nations Internet Governance Forum*, 2020, [https://direitosnarede.org.br/2020/11/17/open-letter-from-brazilian-civil-society-on-the-occasion-of-the-15th-edition-of-the-united-nations-internet-governance-forum/]

CPO Magazine, 2020, [https://www.cpomagazine.com/cyber-security/brazils-health-ministrys-website-data-leak-exposed-243-million-medical-records-for-more-than-6-months/]

DIAMOND L., "Facing Up to the Democratic Recession", *Journal of Democracy,* Vol. 26(1), 2015

DIAMOND L., *Ill Winds: Saving democracy from Russian rage, Chinese ambition, and American complacency*, Penguin Press, 2019

DIAS T., R.M. MARTINS, "Documentos vazados mostram que ABIN pediu ao SERPRO dados e fotos de todas as CNHS do país", *The Intercept Brasil*, 2020 [https://theintercept.com/2020/06/06/abin-carteira-motorista-serpro-vigilancia/]

GINSBURG T., A.Z. HUQ, *How to Save a Constitutional Democracy*, The University of Chicago Press, 2018

HOWARD P.N., *Lie Machines: How to save democracy from troll armies, deceitful robots, junk news operations, and political operatives*, Yale University Press, 2020

KEMENY R., "Brazil is sliding into techno-authoritarianism", *MIT Technology Review*, 2020

[https://www.technologyreview.com/2020/08/19/1007094/brazil-bolsonaro-data-privacy-cadastro-base/]

LANZA E., *Standards for a Free, Open and Inclusive Internet*, OAS, 2017 [http://www.oas.org/en/iachr/expression/docs/publications/INTERNET_2016_ENG.pdf].

LARUE F. *et al*, *Joint Declaration on Freedom of Expression and the Internet*, Inter-American Commission on Human Rights, 2011 [http://www.oas.org/en/iachr/expression/showarticle.asp?artID=849&lID=1]

LEVITSKY S., D. ZIBLATT, *How Democracies Die*, Crown, 2018

LEVITSKY S., L. WAY, "The Myth of Democratic Recession", *Journal of Democracy,* Vol. 26(1), 2015.

MARGETTS H., "Political Behavior and the Acoustics of Social Media", *Nature Human Behavior,* Vol. 1(86), 2017

MARGETTS H., "Rethinking Democracy with Social Media", in A. GAMBLE and T. WRIGHT (eds.), *Political Quarterly Monograph Series*, 2019

MCCOY T., "An investigation into fake news targets Brazil's Bolsonaros, and critics fear a constitutional crisis", *The Washington Post*, 2020 [https://www.washingtonpost.com/world/the_americas/brazil-bolsonaro-fake-news-coronavirus/2020/06/03/60194428-a4de-11ea-898e-b21b9a83f792_story.html]

MELLO P.C., *A Máquina do Ódio: notas de uma repórter sobre fake news e violência digital*, Companhia das Letras, 2020

MONCAU L.F.M., D.W. ARGUELHES, "The Marco Civil da Internet and Digital Constitutionalism", in G. FROSIO, *Oxford Handbook of Online Intermediary Liability*, 2020

Provisional Measure No. 869 of 2018, amending Law No. 13.709/2018 to provide for the protection of personal data and create the National Data Protection Authority [https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/135062]

RYAN-MOSLEY T., "'It's been really, really bad': How Hispanic voters are being targeted by disinformation", *MIT Technology Review*, 2020 [https://www.technologyreview.com/2020/10/12/1010061/hispanic-voter-political-targeting-facebook-whatsapp/].

SESIN C., "Did Trump draw out a new Latino Republican voter bloc in Florida?", *NBC News*, 2020 [https://www.nbcnews.com/news/latino/did-trump-draw-out-new-latino-republican-voter-bloc-florida-n1248577]

SCHEPPELE K. L., "The Rule of Law and the Frankenstate: Why governance checklists do not work", *Governance*, No. 26, 2013

SCHEPPELE K.L., "Worst Practices and the Transnational Legal Order (or How to Build a Constitutional 'Democratorship' in Plain Sight)", University of Toronto Faculty of Law Working Paper, 2016
[https://www.law.utoronto.ca/utfl_file/count/documents/events/wright-scheppele2016.pdf]

SCHREIBER M., "Coronavírus: uso de dados de geolocalização contra a pandemia põe em risco sua Privacidade?", BBC News Brazil, 2020,
[https://www.bbc.com/portuguese/brasil-52357879]

Scott A. Hale *et al*, "How Digital Design Shapes Political Participation: A natural experiment with social information*"*, *PLoS ONE Journal,* Vol. 13(4), 2018

SOUZA C.A., M. VIOLA and R. LEMOS (eds.), *Brazil's Internet Bill of Rights: A Closer Look*., Second Edition, 2017, p. 41
[https://itsrio.org/wp-content/uploads/2018/02/v5_com-capa__pages_miolo_Brazil-Internet-Bill-of-Rights-A-closer-Look.pdf]

TARDÁGUILA C., "*How techno-populists put the 'Hate Machine' to work in spreading disinformation"*, Poynter, 2020,
[https://www.poynter.org/fact-checking/2020/how-techno-populists-put-the-hate-machine-to-work-in-spreading-disinformation/]

The Guardian, 2018
[https://www.theguardian.com/world/2018/dec/23/maria-do-rosario-jair-bolsonaro-brazil-rape]

URBINATI N., "A Revolt against Intermediary Bodies", *Constellations*, Vol. 22, 2015

VALENTE R., "Relatório do governo separa em grupos jornalistas e influenciadores", *UOL Notícias*, 2020
[https://noticias.uol.com.br/colunas/rubens-valente/2020/12/01/governo-bolsonaro-jornalistas-redes-sociais.htm]

World Wide Web Foundation, *Welcoming Brazil's Marco Civil: A World First Digital Bill of Rights*, 2014
[https://webfoundation.org/2014/03/welcoming-brazils-marco-civil-a-world-first-digital-bill-of-rights/]