THE RIGHT TO DATA PROTECTION VERSUS "SECURITY": CONTRADICTIONS OF THE RIGHTS-DISCOURSE IN THE BRAZILIAN GENERAL PERSONAL DATA PROTECTION ACT (LGPD)

O DIREITO À PROTEÇÃO DE DADOS VERSUS "SEGURANÇA": CONTRADIÇÕES DA RETÓRICA DE DIREITOS NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

Marcos Vinicius Viana da Silva[I]
Erick da Luz Scherf[II]
José Everton da Silva[III]

[I] University of Vale do Itajaí (UNIVALI), Balneário Camboriú, SC, Brazil. Doctor of Law. Email: vianaesilvaproducoes@gmail.com

[II] University of Vale do Itajaí (UNIVALI), Balneário Camboriú, SC, Brazil. E-mail: erickscherf@gmail.com

[III] University of Vale do Itajaí (UNIVALI), Balneário Camboriú, SC, Brazil. Doctorate in Legal Science. E-mail: caminha@univali.br

DOI: 10.20912/rdc.v15i36.18

Autores convidados

Abstract: The protection of personal data in the cyberspace has been an issue of concern for quite some time. However, with the revolutions in information technology, big data and the internet of things, data privacy protection has become paramount in an era of free information flows. Considering this context, this research intends to shine a light on the experience of Brazil regarding data privacy protection, through the analysis of a brand new bill passed by Congress: the Brazilian General Personal Data Protection Act. Our assessment of the legislation was made from the perspective of a human rights-based approach to data, aiming to analyze both advancements, limitations and contradictions of the rights-discourse in the LGPD. Our main conclusions were that the (public and national) security rhetoric, also present in the bill, can create a state of exception regarding the processing of personal data of those considered "enemies of the state", which may result in violations of fundamental rights and procedural guarantees.

Keywords: Data Privacy. Human Rights. Digital Age. Security.

Resumo: A proteção de dados pessoais no ciberespaço é motivo de preocupação há bastante tempo. No entanto, com as revoluções na tecnologia da informação, big data e internet das coisas, a proteção da privacidade de dados se tornou fundamental em uma era de fluxos livres de informações. Considerando esse contexto, esta

Revista Direitos Culturais | Santo Ângelo | v. 15 | n. 36 | p. 209-232 | maio/agos. 2020
DOI: http://dx.doi.org/10.20912/rdc.v15i36.18

pesquisa pretende esclarecer a experiência do Brasil em relação à proteção da privacidade de dados pessoais, através da análise da recente Lei Geral de Proteção de Dados Pessoais (LGPD). Nossa avaliação da legislação foi feita a partir da perspectiva de uma abordagem aos dados embasada nos direitos humanos, com o objetivo de analisar os avanços, limitações e contradições da retórica dos direitos na LGPD. Nossas principais conclusões foram de que a retórica da segurança (pública e nacional), também presente na Legislação, pode criar uma espécie de estado de exceção no que concerne ao tratamento de dados pessoais daqueles considerados "inimigos do Estado", o que pode resultar em violações de direitos humanos e de garantias processuais fundamentais.

Palavras-chave: Privacidade de Dados. Direitos Humanos. Era Digital. Segurança.

Introduction

The protection of personal data in the cyberspace[1] has been an issue of concern maybe since the invention of the internet[2], however, preoccupations have increased in the last decades since the rise of big data[3] and other new sources and methods for large-scale data analysis

1 Cyberspace, according to the Cambridge Dictionary (Online), can be defined as "an electronic system that allows computer users around the world to communicate with each other or to access information for any purpose". *In*: CAMBRIDGE UNIVERSITY PRESS (CUP). *Cambridge Dictionary***.** Online: CUP, 2019. Available from: https://dictionary.cambridge.org/dictionary/english/cyberspace. Access on: 26 Aug. 2019. Online, n.p.

2 "The first recorded description of the social interactions that could be enabled through networking was a series of memos written by J.C.R. Licklider of MIT in August 1962 discussing his "Galactic Network" concept. He envisioned a globally interconnected set of computers through which everyone could quickly access data and programs from any site. In spirit, the concept was very much like the Internet of today". *In*: INTERNET SOCIETY. *Brief History of the Internet.* 1997. Available from: https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf. Access on: 26 Aug. 2019. Online, n.p.

3 MENNECKE, Brian *et al. Privacy in the Age of Big Data:* The Challenges and Opportunities for Privacy Research. 2014. Thirty Fifth International Conference on Information Systems. Available from: https://pdfs.semanticscholar.org/a91d/3732d577d0c2078acac88c6da1bb48cc5ca6.pdf. Access on: 26 Aug. 2019.

which are "[…] likely to have far-reaching implications for the future of privacy"[4].

Nevertheless, issues of information privacy are far from new. As France Bélanger and Robert E. Crossler report, "the concept of information privacy existed long before information and communication technologies changed its occurrences, impacts, and management"[5].

However, emerging technologies in the field of Information Systems (IS) and beyond – embedded in the context of a Digital and Technological Age – seem to have changed considerably how information is produced and shared, causing known and yet to be known impacts on data privacy:

> At present – when most information is spread and carried on in a digital form, when communication technologies such as smartphones and free internet access ubiquity have become part of daily life, when commerce, health and financial services, education and entertainment, social platforms and infrastructures are provided online and in real-time – contemporary life is increasingly moving in the direction of becoming a "transparent society". Information technologies and computing systems that record our every keystroke and physical movement are dissolving the borders between the individual, state and private enterprise[6].

In the light of these concerns, on October 2018, the United Nations (UN) High-Level Committee on Management has adopted the "*Personal Data Protection and Privacy Principles"*, which shows that international institutions are also worried about the future of

4 ALTMAN, Micah *et al*. Practical approaches to big data privacy over time. *International Data Privacy Law*, [*S.l.*], v. 8, n. 1, p. 29-51, 1 Feb. 2018. Oxford University Press (OUP). Available from: http://dx.doi.org/10.1093/idpl/ipx027. Access on: 26 Aug. 2019., p. 3.

5 BÉLANGER, France; CROSSLER, Robert E. Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, [*S.l.*], v. 35, n. 4, p. 1017-1042, 2011. Available from: http://dx.doi.org/10.2307/41409971. Access on: 26 Aug. 2019., p. 1017.

6 DAMEN, Juliane; KÖHLER, Lena; WOODARD, Sean. *The Human Right of Privacy in the Digital Age*. 2018. Universitätsverlag Potsdam. Available from: https://publishup.uni-potsdam.de/opus4-ubp/frontdoor/deliver/index/docId/39926/file/srp03.pdf. Access on: 26 Aug. 2019., p. 1.

Revista Direitos Culturais | Santo Ângelo | v. 15 | n. 36 | p. 209-232 | maio/agos. 2020
DOI: http://dx.doi.org/10.20912/rdc.v15i36.18

information regulation at an international level, as the Principles aim to: (i) harmonize standards for the protection of personal data across the United Nations System; (ii) facilitate the accountable processing of personal data for the purposes of implementing the mandates of the UN; and (iii) ensure respect for the human rights and fundamental freedoms of individuals, in particular the right to privacy[7].

Indeed, with the revolutions in information technology, big data and the internet of things[8], data privacy has become an issue of concern to individuals, enterprises, governments, international organizations and many other actors from different social and geographical backgrounds[9]. In this sense, the main regulatory mark concerning data privacy often cited as referential nowadays - even though many countries have pushed legislation on the matter - has been the European Union (EU) "*General Data Protection Regulation"* (GDPR). The GDPR was approved by the EU Parliament on 14 April 2016 and entered into force on 25 May 2018, aiming at (a) harmonizing data privacy laws across Europe; (b) protecting and empowering all EU citizens' data privacy; and (c) reshaping the way organizations across the region approach data privacy[10].

7 UN. *PERSONAL DATA PROTECTION AND PRIVACY PRINCIPLES.* 2018. Available from: https://www.unsceb.org/CEBPublicFiles/UN-Principles-on-Personal-Data-Protection-Privacy-2018.pdf. Access on: 27 Aug. 2019.

8 BOSUA, Rachelle *et al*. *Privacy in a world of the Internet of Things*: A Legal and Regulatory Perspective. 2017. Networked Society Institute at University of Melbourne. Available from: https://networkedsociety.unimelb.edu.au/__data/assets/pdf_file/0008/2640779/IoT-and-privacy-NSI-Disc-6.pdf. Access on: 27 Aug. 2019.

9 "Given the rapid changes in communications, technology and the exchange and use of data in emerging economies across the world, research is urgently needed on the state of data protection in partner countries, and on comparable regulatory standards and best practices". *In*: PRIVACY INTERNATIONAL. *Privacy in the developing world*: a global research agenda. 2012. Available from: https://privacyinternational.org/blog/1456/privacy-developing-world-global-research-agenda. Access on: 27 Aug. 2019. Online, n.p.

10 EUROPEAN COMMISSION. *EU data protection rules*: Stronger rules on data protection mean people have more control over their personal data and businesses benefit from a level playing field. 2018. Available from: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-

However, as Europe and the US have been the main focus of studies regarding data privacy, other regions of the globe have often been neglected by scholars in the fields of IS, IT, Privacy Law, among others. Because differently from the US or the European countries, other regions across the globe have had less experience with data regulation as well as they did not necessarily make data privacy protection a priority of their policy-making agendas, even though legislation on data privacy and protection has spread across the world. Developing countries, for an example, "[…] venture into new technologies without understanding the implications and the legal frameworks under which the technologies operate […]" and "[…] the technological pace keeps accelerating while the legal pace remains particularly slow. For this reason, developing countries may not effectively deal with crimes committed over the internet or in the office work environment"[11].

Taking this context into consideration, this research intends to shine a light on the experience of Brazil regarding data privacy protection, through the analysis of a brand new legislation approved by Congress: the Brazilian General Personal Data Protection Act (*Lei Geral de Proteção de Dados Pessoais*, in Brazilian Portuguese) (hereinafter referred as "LGPD", or as the "Act"). As Brazil has been taking steps towards the digital transformation of government and the public sector[12], as well as has developed several national plans around the transformation into a digital economy[13], issues of data privacy and

reform-eu-data-protection-rules_en. Access on: 27 Aug. 2019.

11 TOVI, Muli David; MUTHAMA, Mutua Nicholas. ADDRESSING THE CHALLENGES OF DATA PROTECTION IN DEVELOPING COUNTRIES. *European Journal of Computer Science and Information Technology*, [*S.l.*], v. 1, n. 2, p. 1-9, Sept. 2013., p. 1.

12 OECD. *Digital Government Review of Brazil*: Towards the Digital Transformation of the Public Sector. Paris: OECD Publishing, 2018. Available from: https://doi.org/10.1787/9789264307636-en. Access on: 27 Aug. 2019.

13 MAREGA, Patricia. *BRAZIL DIGITAL ECONOMY INITIATIVES*. 2017. Available from:https://www.export.gov/article?id=Brazil-Digital-Economy-Initiatives. Access on: 27 Aug. 2019.

Revista Direitos Culturais | Santo Ângelo | v. 15 | n. 36 | p. 209-232 | maio/agos. 2020
DOI: http://dx.doi.org/10.20912/rdc.v15i36.18

protection are in *L'Ordre du jour* of politicians, policy-makers and scholars on the field.

Considering that, as well as the fact that the Act has incorporated the rights-talk into its main text, our objective is to analyze both advancements, limitations and contradictions of the rights-discourse in the LGPD. Our secondary goal is to demonstrate how the security speech, also present in the bill's text, may undermine the rights enshrined in the legislation itself. The research endows a qualitative approach alongside a review of literature and text-analysis, our main theoretical starting point is the human rights-based approach to data.

1 The Extent of the Human Right to Data Protection in the Digital Age

Way before discussions surrounding a so-called "human right to data privacy" arise, scholars and policymakers were already worried about issues of privacy in the Information/Digital Age. Daniel J. Solove, in his book "*The Digital Person: Technology and Privacy in the Information Age*" published in 2004, argues how the existing law protecting information privacy for an example, has not adequately responded to the emergence of digital dossiers and other types of information technology[14]. Thus, the author implied an urgent need to rethink privacy in the Information Age.

However, in light of the rapid advancements on digital technologies, privacy-related problems have gained even more attention nowadays. Carly Nyst and Tomaso Falchetta argue that "recent years have seen the right to privacy, particularly as it pertains to the surveillance and interception of communications, transform from a much-neglected human rights issue to the focus of multiple UN General Assembly and Human Rights Council resolution"[15]. Much of that is

14 SOLOVE, Daniel J. *The Digital Person:* Technology and Privacy in the Information Age. New York: New York University Press, 2004.

15 NYST, Carly; FALCHETTA, Tomaso. The Right to Privacy in the Digital

due to the rise and expansion of the internet and the advancement of information and digital technologies, which have a major impact on the right to privacy worldwide. Nevertheless, within this context, the question of data privacy has become a major concern, as pointed out by members of the Pirate Parties International (PPI), a non-profit international non-governmental organization with consultation status at the UN Economic and Social Council:

> Often without our awareness or consent, detection devices track our movements, our preferences, and any information they are capable of mining from our digital existence. This data is used to manipulate us, rob from us, and engage in prejudice against us- at times legally. We are stalked by algorithms that profile all of us. This is not a dystopian outlook on the future or paranoia. This is present day reality, whereby we live in a data-driven society with ubiquitous corruption that enables a small number of individuals to transgress a destitute mass of phone and internet media users[16].

Therefore, many legal scholars in the field of privacy law and human rights, as well as constitutional courts and international institutions have argued for the acknowledgement/existence of data privacy protection as a human right.

First, we must acknowledge that the very concept of data protection is a much-debated one; however, in terms of this paper, we shall consider data protection "*as referring to [the] set of legal rules that aims to protect the rights, freedoms, and interests of individuals, whose personal data are collected, stored, processed, disseminated, destroyed, etc*."[17]

Age. *Journal of Human Rights Practice*, [*S.l.*], v. 9, n. 1, p.104-118, Feb. 2017. Oxford University Press (OUP). Available from: http://dx.doi.org/10.1093/jhuman/huw026. Access on: 02 Sep. 2019., p. 1.

16 GOLDSTEIN, Keith; TOV, Ohad Shem; PRAZERES, Dan. *The Right to Privacy in the Digital Age*. 2018. Presented on behalf of Pirate Parties International Headquarters, a UN ECOSOC Consultative Member, for the Report of the High Commissioner for Human Rights. Available from: https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/PiratePartiesInternational.pdf. Access on: 02 Sep. 2019., Online, n.p.

17 TZANOU, M. Data protection as a fundamental right next to privacy?

Revista Direitos Culturais | Santo Ângelo | v. 15 | n. 36 | p. 209-232 | maio/agos. 2020
DOI: http://dx.doi.org/10.20912/rdc.v15i36.18

Thus, data privacy and protection can be understood as a right autonomous unto itself, apart from the long-time established right to privacy[18], because "data protection seems to fall into the aspect of privacy that is known as control over personal information"[19].

Thus, even though the right to privacy and the right to data protection can indeed interact in a variety of ways, data protection has its own identity[20]. In the European Union (EU) Law for an example, "data protection has been enshrined as a fundamental right, alongside privacy, in the EU Charter of Fundamental Rights, which constitutes primary EU law". While in the context of international human rights law:

> Data protection law is rooted in international human rights instruments such as the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) that protect the right to private life, family life, the home, and correspondence. In particular, the ICCPR has been interpreted by the UN Human Rights Commission (General Comment 16) to include certain data protection guarantees. The only UN instrument dealing specifically with data protection is the set of non-binding UN Guidelines for the regulation of computerized personal data files, dating from 1990. The international treaty in this field with the most States Parties is Council of Europe Convention 108, while a number of other international organizations (such as APEC, the OECD, ECOWAS, and the Organization of American States) have

'Reconstructing' a not so new right. *International Data Privacy Law*, [*S.l.*], v. 3, n. 2, p. 88-99, 20 Mar. 2013. Oxford University Press (OUP). Available from: http://dx.doi.org/10.1093/idpl/ipt004. Access on: 03 Sep. 2019., p. 89. Our italics.

18 See: HENDRICKS, Even; HAYDEN, Trudy; NOVIK, Jack D. *Your right to privacy*: a basic guide to legal rights in an information society. 2. ed. United States of America: Southern Illinois University Press; American Civil Liberties Union, 1990.

19 TZANOU, M. Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. *International Data Privacy Law*, [*S.l.*], v. 3, n. 2, p. 88-99, 20 Mar. 2013. Oxford University Press (OUP). Available from: http://dx.doi.org/10.1093/idpl/ipt004. Access on: 03 Sep. 2019., p. 89.

20 KITTICHAISAREE, Kriangsak; KUNER, Christopher. *The Growing Importance of Data Protection in Public International Law*. 2015. Blog of the European Journal of International Law. Available from: https://www.ejiltalk.org/the-growing-importance-of-data-protection-in-public-international-law/. Access on: 03 Sep. 2019.

adopted data protection instruments, most of which are non-binding[21].

Because most of these international instruments regarding data protection are non-binding, one may think that data protection as an autonomous human right in international human rights law may not exist. Such disagreement also exists regarding other candidates to a "human right" position, let us take for an example the human right to a clean or healthy environment. Many authors defend that the right to a clean environment would not acquire the normativity it needs by simply being drawn from already established human rights[22], while others believe that the right to a clean and healthy environment is already recognized by international law, deriving from different sources such as soft or customary law, and it has also been encrypted in the constitutional law of many countries[23]. Such debate takes place maybe because authors are trying to create a division of labor in International Human Rights Law, between "hard" and "soft" sources of law, when in reality, such sources often intersect each other and a balance between the two is believed to be the most suitable solution for the relative "inefficacy" of non-binding human rights instruments[24].

21 KITTICHAISAREE, Kriangsak; KUNER, Christopher. *The Growing Importance of Data Protection in Public International Law*. 2015. Blog of the European Journal of International Law. Available from: https://www.ejiltalk.org/the-growing-importance-of-data-protection-in-public-international-law/. Access on: 03 Sep. 2019., Online, n.p.

22 FITZMAURICE, Malgosia; MARSHALL, Jill. The Human Right to a Clean Environment – Phantom or Reality? The European Court of Human Rights and English Courts Perspective on Balancing Rights in Environmental Cases. *Nordic Journal of International Law*, [*S.l.*], v. 76, n. 2-3, p. 103-151, 2007. Brill. Available from: http://dx.doi.org/10.1163/090273507x225729. Access at: 03 Sep. 2019.

23 BOYD, David R. Catalyst for Change: Evaluating Forty Years of Experience in Implementing the Right to a Healthy Environment. In: KNOX, John H.; PEJAN, Ramin (Ed.). *The Human Right to a Healthy Environment.* Cambridge: Cambridge University Press, 2018. p. 17-41.

24 CHOUDHURY, Barnali. BALANCING SOFT AND HARD LAW FOR BUSINESS AND HUMAN RIGHTS. *International and Comparative Law Quarterly*, [*S.l.*], v. 67, n. 4, p.961-986, 9 July 2018. Cambridge University Press (CUP). Available from: http://dx.doi.org/10.1017/s0020589318000155. Access on: 03 Sep. 2019.

Revista Direitos Culturais | Santo Ângelo | v. 15 | n. 36 | p. 209-232 | maio/agos. 2020
DOI: http://dx.doi.org/10.20912/rdc.v15i36.18

From our point of view, the discussion should focus on how to enforce the existing legal mechanisms and instruments (binding or non-binding) set out to protect personal data rather than aiming at building up new ones. Bart van der Sloot provides a very interesting critical approach to the EU General Data Protection Regulation for an example. According to him, "the Regulation proposes introducing a number of specific obligations and rights in order to protect the interests of citizens and consumers and provides far-reaching powers for governmental agencies to enforce these rules"[25], however, he points out that "*this is directly against the original purpose of and rationale behind data protection rules and, moreover, an increased emphasis on consumer interests and rights to control personal data seems like an inadequate tool for solving the current problems involved with Big Data*"[26].

Therefore, we should make an effort to examine already existing legislation, with the purpose of exploring both advancements and limitations to data protection regulations from different socio-geographical backgrounds. With that in mind, our goal is to explore how the rights-talk in the Brazilian LGPD may be undermined by the security discourse, permissible under the bill's text. The intent is to explore how securitization moves attempt to justify a state of exception regarding data manipulation and what outcomes it can produce on data privacy and protection.

25 SLOOT, B. van Der. Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation. *International Data Privacy Law*, [*S.l.*], v. 4, n. 4, p.307-325, 3 July 2014. Oxford University Press (OUP). Available from: http://dx.doi.org/10.1093/idpl/ipu014. Access on: 03 Sep. 2019., p. 307.

26 SLOOT, B. van Der. Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation. *International Data Privacy Law*, [*S.l.*], v. 4, n. 4, p.307-325, 3 July 2014. Oxford University Press (OUP). Available from: http://dx.doi.org/10.1093/idpl/ipu014. Access on: 03 Sep. 2019., p. 307. Our italics.

2 Security versus Data Privacy? Bargaining Values and Rights

Privacy is a value many societies cultivate and try to protect, due to many reasons: "tension over privacy is a universal feature of social life […] [,] for it is impossible to imagine a social world where people are indifferent to the potential consequences of sharing information about themselves that only they know"[27]. However, it does not mean that privacy as both a value and a human right has not been subjected to relativization by a variety of social actors for different reasons; one particular clash takes place between issues of security and privacy.

Even though security is a contested concept, taking into account the aims of this paper, we shall consider security as the implementation of privacy's choices: "*security determines who actually can access, use, and alter data […] [;] security, therefore, is the interface layer between information and privacy. It mediates privacy rights, putting them into effect*"[28]. In this sense, we intend to take a closer look at what allegedly "legitimates" data protection breaches, from a security perspective, and how it may undermine privacy protection systems.

Data protection as any other human right is not absolute nor untouchable. It has been long established that rights may be legitimately undermined in various situations, especially when such rights collide, for that exists various legal interpretation theories and principles, such as the proportionality one[29]. The same happens to data privacy, as in many cases personal data and information can indeed be disclosed if it serves a "public interest"; *i.e*., "much as domains of privacy are indispensable for a full and decent life, we also rely on the vitality of

27 RULE, James B. *Privacy in peril.* Oxford: Oxford University Press, 2007., p. 3.

28 BAMBAUER, Derek E. Privacy versus Security. *Journal of Criminal Law and Criminology*, [*S.l*], v. 103, n. 3, p.667-684, 2013. Available from: https://scholarlycommons.law.northwestern.edu/jclc/vol103/iss3/2/. Access on: 05 Sep. 2019., p. 676. Our italics.

29 FORTMAN, Bas de Gaay; MARTENS, Kurt; SALIH, M. A. Mohamed (Ed.). *Hermeneutics, Scriptural Politics, and Human Rights*: Between Text and Context. New York: Palgrave Macmillan, 2009.

Revista Direitos Culturais | Santo Ângelo | v. 15 | n. 36 | p. 209-232 | maio/agos. 2020
DOI: http://dx.doi.org/10.20912/rdc.v15i36.18

what one might term the ‘‘public sphere’’—the realm of actions taken or information offered in public and understood as such by all parties”[30].

However, personal data can also be subjected to invasion, usually by governments, especially when issues of “public security” are at stake, which can result in human rights violations that should not be defensible: “*in controversies over law enforcement or national security, for example, many hold that the most personal information may properly be extracted from unwilling individuals, even by stealth or torture, given the high collective benefits of stopping terrorism or curtailing crime*”[31]. Such disclosure of personal information - under the excuse of “public security” or counterterrorism for an example - if done without external overlook or legal and ethical frameworks, may undermine legal protections of individuals and it can create a state of exception where the state acts without reverence to the law.

One recent legislation in the United Kingdom (UK) has generated quite some buzz around this subject. On 29 November 2016, the Investigatory Powers Act received Royal Assent and entered into force; the Act aims to “provide a new framework to govern the use and oversight of investigatory powers by law enforcement and the security and intelligence agencies”[32]. However, activists have pointed out that the “*Snoopers’ Charter”,* as it has been called, “*introduced the most draconian surveillance regime of any democracy in history*. It lets the authorities hack thousands of devices *en masse*, forces internet providers to collect our browsing histories and make them available to dozens of public bodies”[33]. In mid-2019, civil rights organizations have contested the Act in the High Court of England and Wales, arguing that

30 RULE, James B. *Privacy in peril.* Oxford: Oxford University Press, 2007., p. 8.

31 RULE, James B. *Privacy in peril.* Oxford: Oxford University Press, 2007., p. 12.

32 Government of UK. *Investigatory Powers Act.* 2016. Department of Home Office. Available from: https://www.gov.uk/government/collections/investigatory-powers-bill. Access on: 10 Sep. 2019. Online, n.p.

33 LIBERTY. *COUNTERING TERRORISM*. 2019. Available from: https://www.libertyhumanrights.org.uk/human-rights/countering-terrorism. Access on: 10 Sep. 2019. Online, n.p. Our italics.

"'bulk hacking' powers exploited by the intelligence services to access electronic devices represent an illegal intrusion into the private lives of millions of people"[34].

Notwithstanding, the Brazilian General Personal Data Protection Act (LGPD) has also introduced the debate of data privacy versus security; however, little attention has been given on the subject so far. Thus, our intent is to contest parts of the bill that may have opened space for data privacy breaches under "security" reasons. We apply the human-rights approach to data to investigate what inconsistencies the LGPD present regarding data protection efforts.

3 Contradictions of the Rights-Discourse in the Brazilian Personal Data Protection Act

Firstly, we shall begin by explaining what is a "human rights-approach to data". Secondly, we ought to elucidate the general features of the LGPD and what are the inconsistencies it presents regarding data protection efforts.

Considering the fact that data protection has been acknowledged as a human right both by international and constitutional law(s), as well as it has become the focus of multiple UN General Assembly and Human Rights Council resolutions, the Office of the United Nations High Commissioner for Human Rights (OHCHR) has launched, with the help of numerous human rights experts and organizations, a Human Rights-Based Approach to Data (HRBAD) document[35]. The HRBAD can be defined, according to the OHCHR, "[…] *as the use of data and statistics consistently with international human rights norms*

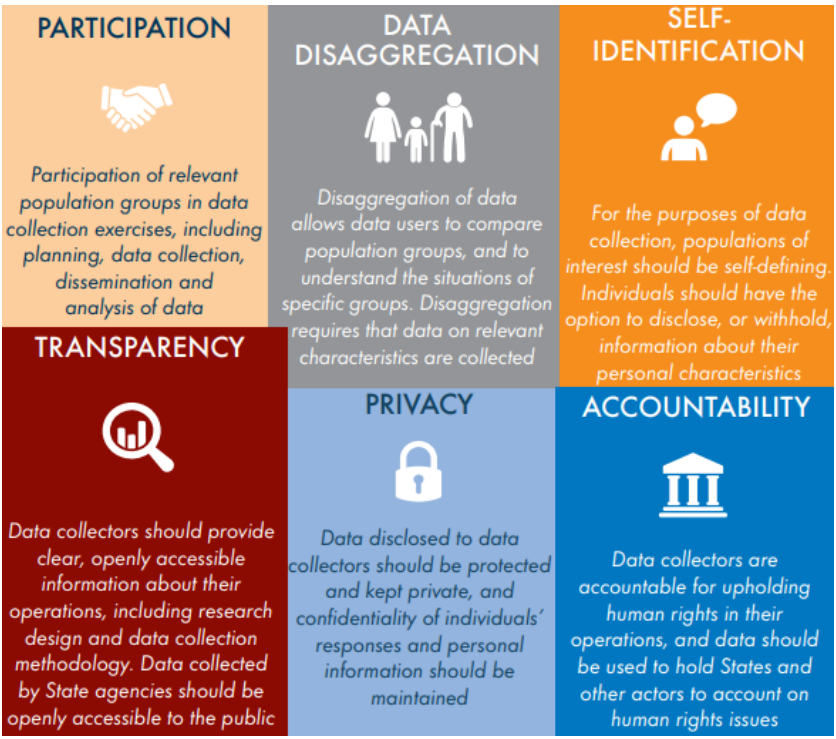
34 BOWCOTT, Owen. 'Bulk hacking' by UK spy agencies is illegal, high court told. *The Guardian*. Online, n.p., jun. 2019. Available from: https://www.theguardian.com/technology/2019/jun/17/liberty-mounts-latest-court-challenge-to-snoopers-charter-mi5-gchq. Access on: 10 Sep. 2019. Online, n.p.

35 The document can be found online on the following link: https://www.ohchr.org/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf.

Revista Direitos Culturais | Santo Ângelo | v. 15 | n. 36 | p. 209-232 | maio/agos. 2020
DOI: http://dx.doi.org/10.20912/rdc.v15i36.18

and principles"[36]. The OHCHR elected six principles as the most important ones regarding data collection: *i.e.*, 1) Participation; 2) Data disaggregation; 3) Self-identification; 4) Transparency; 5) Privacy and 6) Accountability (see Figure 2).

Figure 2 - United Nations Human Rights-Based Approach to Data principles outlined.



Source: OHCHR (2018, Online). Adapted by the authors.

However, despite the fact there is an extensive literature on human rights-based approaches to a variety of human needs and social problems, so far little work has been done on the strengths and

36 OFFICE OF THE UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS (OHCHR). *A HUMAN RIGHTS-BASED APPROACH TO DATA*: LEAVING NO ONE BEHIND IN THE 2030 AGENDA FOR SUSTAINABLE DEVELOPMENT. 2018. Available from: https://www.ohchr.org/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf. Access on: 10 Sep. 2019. p. 2.

weaknesses of a human rights-based approach to data. Alessandro Mantelero builds up a model centered on human rights, called "Human Rights, Ethical and Social Impact Assessment" (HRESIA), which intends to […] *force data controllers to go beyond the traditional focus on data quality and security, and consider the impact of data processing on fundamental rights and collective social and ethical values*"[37].

We believe that this enterprise, alongside the HRBAD, may be able to provide "[…] tools to assess the impacts of data processing on the fundamental rights and freedoms protected by legislators (e.g. GDPR)"[38] on a broader scope, aligned with ideals of social justice and taking into consideration other consequences of data processing on individuals as well as upon society. However, Mantelero's model will not be assessed on this article, because according to the author, the model is still in construction and "a more detailed description of the model and the content of the questionnaire will be discussed in a future publication drawing on the ongoing research"[39].

Firstly, we must draw upon the main features of the Act. Bill no. 13.709, known as the General Personal Data Protection Act (LGPD), was sanctioned by former president Michel Temer in August 2018 and will enter into force in August 2020. Its purpose is to regulate the processing of personal data of customers and users of public and private companies[40]: "the legislation - similar to the General Data Protection

37 MANTELERO, Alessandro. AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. *Computer Law & Security Review*, [*S.l.*], v. 34, n. 4, p. 754-772, ago. 2018. Elsevier BV. Available from: http://dx.doi.org/10.1016/j.clsr.2018.05.017. Access on: 11 Sep. 2019., p. 754.

38 MANTELERO, Alessandro. AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. *Computer Law & Security Review*, [*S.l.*], v. 34, n. 4, p. 754-772, ago. 2018. Elsevier BV. Available from: http://dx.doi.org/10.1016/j.clsr.2018.05.017. Access on: 11 Sep. 2019., p. 772.

39 MANTELERO, Alessandro. AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. *Computer Law & Security Review*, [*S.l.*], v. 34, n. 4, p. 754-772, ago. 2018. Elsevier BV. Available from: http://dx.doi.org/10.1016/j.clsr.2018.05.017. Access on: 11 Sep. 2019., p. 754.

40 PASSARELLI, Vinícius. LGPD: entenda o que é a Lei Geral de Proteção de Dados Pessoais. **O Estadão**. Online, n.p. 31 May 2019. Available from: https://

Revista Direitos Culturais | Santo Ângelo | v. 15 | n. 36 | p. 209-232 | maio/agos. 2020
DOI: http://dx.doi.org/10.20912/rdc.v15i36.18

Regulation (GDPR) - creates a new legal framework for the use of personal data processed on or related to individuals in Brazil, regardless of where the data processor is located"[41].

According to the Preliminary Provisions of the LGPD: "*Art. 1 This Law provides for the processing of personal data, including by digital means, by a natural person or a legal entity of public or private law, with the purpose of protecting the fundamental rights of freedom and privacy and the free development of the personality of the natural person*"[42]. Chris Brook reminds us that "prior to the LGPD's passage, data protection in Brazil was primarily enforced via a collection of frameworks, including the country's Civil Rights Framework for the Internet (Internet Act) and Consumer Protection Code"[43]. It means that the LGPD has made a significant contribution towards the creation of a legal framework regarding personal data protection in Brazil. Notwithstanding, the principles which guide the legislation are below described:

Art. 6 Activities of processing of personal data shall be done in good faith and be subject to the following principles:

> I – purpose: processing done for legitimate, specific and explicit purposes of which the data subject is informed, with no possibility of subsequent processing that is incompatible with these purposes;
>
> II – suitability: compatibility of the processing with the purposes communicated to the data subject, in accordance with the context of the processing;

politica.estadao.com.br/blogs/fausto-macedo/lgpd-entenda-o-que-e-a-lei-geral-de-protecao-de-dados-pessoais/. Access on: 11 Sep. 2019.

41 BROOK, Chris. *Breaking Down LGPD, Brazil's New Data Protection Law*. 2019. Digital Guardian. Available from: https://digitalguardian.com/blog/breaking-down-lgpd-brazils-new-data-protection-law. Access on: 11 Sep. 2019.

42 BRASIL. Law nº 13709, August 14 2018. *General Personal Data Protection Act*. Brasília, 2018. Available from: https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf. Access on: 11 Sep. 2019. Translation by Ronaldo Lemos, Daniel Douek, Sofia Lima Franco, Ramon Alberto dos Santos and Natalia Langenegger, Lawyers at Pereira Neto | Macedo Advogados.

43 BROOK, Chris. *Breaking Down LGPD, Brazil's New Data Protection Law*. 2019. Digital Guardian. Available from: https://digitalguardian.com/blog/breaking-down-lgpd-brazils-new-data-protection-law. Access on: 11 Sep. 2019. Online, n.p.

> III - necessity: limitation of the processing to the minimum necessary to achieve its purposes, covering data that are relevant, proportional and non-excessive in relation to the purposes of the data processing;
>
> IV – free access: guarantee to the data subjects of facilitated and free of charge consultation about the form and duration of the processing, as well as about the integrity of their personal data;
>
> V – quality of the data: guarantee to the data subjects of the accuracy, clarity, relevancy and updating of the data, in accordance with the need and for achieving the purpose of the processing;
>
> VI – transparency: guarantee to the data subjects of clear, precise and easily accessible information about the carrying out of the processing and the respective processing agents, subject to commercial and industrial secrecy;
>
> VII – security: use of technical and administrative measures which are able to protect personal data from unauthorized accesses and accidental or unlawful situations of destruction, loss, alteration, communication or dissemination;
>
> VIII – prevention: adoption of measures to prevent the occurrence of damages due to the processing of personal data;
>
> IX – nondiscrimination: impossibility of carrying out the processing for unlawful or abusive discriminatory purposes; and
>
> X – accountability: demonstration by the agent of the adoption of measures which are efficient and capable of proving the compliance with the rules of personal data protection, including the efficacy of such measures.[44]

The LGPD undoubtedly covers a wide range of principles and practices that aim at protecting the fundamental rights of natural persons when activities of personal data processing take place. However, the legislation also opens the possibility for the legitimization of rights violations based on security reasons. Article 4 of the LGPD establishes that: "This Law does not apply to the processing of personal data that: III – is done exclusively for purposes of: a) *public safety*; b) *national defense*; c) *state security*; or d) *activities of investigation and*

44 BRASIL. Law nº 13709, August 14 2018. *General Personal Data Protection Act*. Brasília, 2018. Available from: https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf. Access on: 11 Sep. 2019. Translation by Ronaldo Lemos, Daniel Douek, Sofia Lima Franco, Ramon Alberto dos Santos and Natalia Langenegger, Lawyers at Pereira Neto | Macedo Advogados.

Revista Direitos Culturais | Santo Ângelo | v. 15 | n. 36 | p. 209-232 | maio/agos. 2020
DOI: http://dx.doi.org/10.20912/rdc.v15i36.18

prosecution of criminal offenses […].[45] Considering that, one can say that, under these circumstances (provided on Article 4 of the LGPD), the Brazilian government is thereby authorized to ignore the principles and norms set by the LGPD in order to safeguard ambiguous values of "public security" and "national defense".

Article 4 of the LGPD, therefore, makes room for personal data to be subjected to invasion by the government, which can result in serious human rights violations, especially regarding the procedural guarantees of those considered "enemies of the state". Such disclosure of personal information - under the excuse of "public security" or counterterrorism for an example - undermines legal protections of individuals and creates a state of exception where the government has no reverence to the law. Taking into account the fact that concepts such as "public safety" and "national defense/security" are vague and can mean about anything, legal rights and guarantees can be easily undermined in order to satisfy "security" agendas. As well said by Justice Black in New York Times Co. v. United States (1971): "*the word 'security' is a broad, vague generality whose contours should not be invoked to abrogate the fundamental law embodied in the First Amendment*"[46], nor it should be invoked to abrogate the rights and principles enshrined in the LGPD.

Ultimately, the LGDP completely disregards the fundamental principles covered by the HRBAD when it opens the possibility to data processing actions to take place outside the scope of the law in order to protect the "security" of the state and its people. In its privacy protection principle, the HRBAD establishes that "data that relates to personal characteristics, and in particular sensitive personal characteristics (including but not limited to data on ethnicity, sexual

45 BRASIL. Law nº 13709, August 14 2018. *General Personal Data Protection Act*. Brasília, 2018. Available from: https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf. Access on: 11 Sep. 2019. Translation by Ronaldo Lemos, Daniel Douek, Sofia Lima Franco, Ramon Alberto dos Santos and Natalia Langenegger, Lawyers at Pereira Neto | Macedo Advogados.

46 UNITED STATES. United States Supreme Court. New York Times Co. V. United States nº 403 U.S. 713. *New York Times Co. v. United States (no. 1873)*. [S.l], n.p.

orientation, gender identity or health status) should be handled only with the express consent of the individual concerned"[47]. However, if under security reasons the LGDP consents the state to act in disregard of the privacy protection principle, a pathway to data privacy breaches is opened, and it might not be easily closed.

Concluding Remarks

The protection of personal data in the cyberspace has been an issue of concern for quite some time. However, with the revolutions in information technology, big data and the internet of things, data privacy protection has become paramount in an era of free information flows. Considering this context, this research intended to shine a light on the experience of Brazil regarding data privacy protection, through the analysis of a brand new bill passed by Congress: the Brazilian General Personal Data Protection Act.

Firstly, we looked for the historical and legal aspects of personal data protection, and we realized that many legal scholars in the field of privacy law and human rights, as well as constitutional courts and international institutions have argued for the acknowledgement/ existence of data privacy protection as a human right. Consequently, following the path of Bart van der Sloot in his examination of the GDPR, we made an effort to examine both advancements and limitations of the LGPD regarding personal data protection. Our focus was at exploring how the rights-talk in the Brazilian LGPD may be undermined by the security discourse. The intent was to explore how securitization moves attempt to justify a state of exception regarding data manipulation and what outcomes it can produce on data privacy protection.

47 OHCHR. *A HUMAN RIGHTS-BASED APPROACH TO DATA*: LEAVING NO ONE BEHIND IN THE 2030 AGENDA FOR SUSTAINABLE DEVELOPMENT. 2018. Available from: https://www.ohchr.org/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf. Access on: 10 Sep. 2019. p. 17.

Revista Direitos Culturais | Santo Ângelo | v. 15 | n. 36 | p. 209-232 | maio/agos. 2020
DOI: http://dx.doi.org/10.20912/rdc.v15i36.18

We conclude that, Article 4 of the LGPD makes room for personal data to be subjected to invasion by the government, which can result in serious human rights violations, especially regarding the procedural guarantees of those considered "enemies of the state". Such legitimation of personal data disclosure under the excuse of public or national "security" can undermine legal protections of individuals and create a state of exception where the government has no reverence to the law. Considering the vagueness of "public safety" and "national defense/ security" definitions, we pointed out that legal rights and guarantees can be easily undermined in order to satisfy "security" agendas. Which, ultimately, completely disregards the fundamental principles covered by the HRBAD and the LGPD itself, when the legislator opened the possibility to data processing actions to take place outside the scope of the law under "security" claims.

References

ALTMAN, Micah *et al*. Practical approaches to big data privacy over time. *International Data Privacy Law*, [*S.l.*], v. 8, n. 1, p. 29-51, 1 Feb. 2018. Oxford University Press (OUP). Available from: http://dx.doi.org/10.1093/idpl/ipx027. Access on: 26 Aug. 2019.

BAMBAUER, Derek E.. Privacy versus Security. *Journal of Criminal Law and Criminology*, [*S.l.*], v. 103, n. 3, p. 667-684, 2013. Available from: https://scholarlycommons.law.northwestern.edu/jclc/vol103/iss3/2/. Access on: 05 Sep. 2019.

BÉLANGER, France; CROSSLER, Robert E.. Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, [*S.l.*], v. 35, n. 4, p. 1017-1042, 2011. Available from: http://dx.doi.org/10.2307/41409971. Access on: 26 Aug. 2019.

BOSUA, Rachelle *et al*. *Privacy in a world of the Internet of Things*: A Legal and Regulatory Perspective. 2017. Networked Society Institute at University of Melbourne. Available from: https://networkedsociety.

unimelb.edu.au/__data/assets/pdf_file/0008/2640779/IoT-and-privacy-NSI-Disc-6.pdf. Access on: 27 Aug. 2019.

BOWCOTT, Owen. 'Bulk hacking' by UK spy agencies is illegal, high court told. *The Guardian*. Online, n.p., jun. 2019. Available from: https://www.theguardian.com/technology/2019/jun/17/liberty-mounts-latest-court-challenge-to-snoopers-charter-mi5-gchq. Access on: 10 Sep. 2019.

BOYD, David R.. Catalyst for Change: Evaluating Forty Years of Experience in Implementing the Right to a Healthy Environment. In: KNOX, John H.; PEJAN, Ramin (Ed.). *The Human Right to a Healthy Environment.* Cambridge: Cambridge University Press, 2018. p. 17-41.

BRASIL. Law nº 13709, August 14 2018. *General Personal Data Protection Act*. Brasília, 2018. Available from: https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf. Access on: 11 Sep. 2019. Translation by Ronaldo Lemos, Daniel Douek, Sofia Lima Franco, Ramon Alberto dos Santos and Natalia Langenegger, Lawyers at Pereira Neto | Macedo Advogados.

BROOK, Chris. *Breaking Down LGPD, Brazil's New Data Protection Law*. 2019. Digital Guardian. Available from: https://digitalguardian.com/blog/breaking-down-lgpd-brazils-new-data-protection-law. Access on: 11 Sep. 2019.

CHOUDHURY, Barnali. BALANCING SOFT AND HARD LAW FOR BUSINESS AND HUMAN RIGHTS. *International and Comparative Law Quarterly*, [*S.l.*], v. 67, n. 4, p.961-986, 9 July 2018. Cambridge University Press (CUP). Available from: http://dx.doi.org/10.1017/s0020589318000155. Access on: 03 Sep. 2019.

DAMEN, Juliane; KÖHLER, Lena; WOODARD, Sean. *The Human Right of Privacy in the Digital Age*. 2018. Universitätsverlag Potsdam. Available from: https://publishup.uni-potsdam.de/opus4-ubp/frontdoor/deliver/index/docId/39926/file/srp03.pdf. Access on: 26 Aug. 2019.

EUROPEAN COMMISSION. *EU data protection rules*: Stronger rules on data protection mean people have more control over their personal data and businesses benefit from a level playing field. 2018.

Revista Direitos Culturais | Santo Ângelo | v. 15 | n. 36 | p. 209-232 | maio/agos. 2020
DOI: http://dx.doi.org/10.20912/rdc.v15i36.18

Available from: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en. Access on: 27 Aug. 2019.

FITZMAURICE, Malgosia; MARSHALL, Jill. The Human Right to a Clean Environment – Phantom or Reality? The European Court of Human Rights and English Courts Perspective on Balancing Rights in Environmental Cases. *Nordic Journal of International Law*, [*S.l.*], v. 76, n. 2-3, p. 103-151, 2007. Brill. Available from: http://dx.doi.org/10.1163/090273507x225729. Access on: 03 Sep. 2019.

FORTMAN, Bas de Gaay; MARTENS, Kurt; SALIH, M. A. Mohamed (Ed.). *Hermeneutics, Scriptural Politics, and Human Rights*: Between Text and Context. New York: Palgrave Macmillan, 2009.

GOLDSTEIN, Keith; TOV, Ohad Shem; PRAZERES, Dan. *The Right to Privacy in the Digital Age***.** 2018. Presented on behalf of Pirate Parties International Headquarters, a UN ECOSOC Consultative Member, for the Report of the High Commissioner for Human Rights. Available from: https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/PiratePartiesInternational.pdf. Access on: 02 Sep. 2019.

GOVERNMENT OF UK. *Investigatory Powers Act*. 2016. Department of Home Office. Available from: https://www.gov.uk/government/collections/investigatory-powers-bill. Access on: 10 Sep. 2019.

KITTICHAISAREE, Kriangsak; KUNER, Christopher. *The Growing Importance of Data Protection in Public International Law*. 2015. Blog of the European Journal of International Law. Available from: https://www.ejiltalk.org/the-growing-importance-of-data-protection-in-public-international-law/. Access on: 03 Sep. 2019.

LIBERTY. *COUNTERING TERRORISM*. 2019. Available from: https://www.libertyhumanrights.org.uk/human-rights/countering-terrorism. Access on: 10 Sep. 2019.

MANTELERO, Alessandro. AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. *Computer Law & Security Review*, [*S.l.*], v. 34, n. 4, p. 754-772, ago. 2018. Elsevier BV.

Available from: http://dx.doi.org/10.1016/j.clsr.2018.05.017. Access on: 11 Sep. 2019.

MAREGA, Patricia. *BRAZIL DIGITAL ECONOMY INITIATIVES*. 2017. Available from: https://www.export.gov/article?id=Brazil-Digital-Economy-Initiatives. Access on: 27 Aug. 2019.

MENNECKE, Brian *et al*. *Privacy in the Age of Big Data:* The Challenges and Opportunities for Privacy Research. 2014. Thirty Fifth International Conference on Information Systems. Available from: https://pdfs.semanticscholar.org/a91d/3732d577d0c2078acac88c6da1bb48cc5ca6.pdf. Access on: 26 Aug. 2019.

NYST, Carly; FALCHETTA, Tomaso. The Right to Privacy in the Digital Age. *Journal of Human Rights Practice*, [*S.l.*], v. 9, n. 1, p.104-118, Feb. 2017. Oxford University Press (OUP). Available from: http://dx.doi.org/10.1093/jhuman/huw026. Access on: 02 Sep. 2019.

OECD. *Digital Government Review of Brazil*: Towards the Digital Transformation of the Public Sector. Paris: OECD Publishing, 2018. Available from: https://doi.org/10.1787/9789264307636-en. Access on: 27 Aug. 2019.

OHCHR. *A HUMAN RIGHTS-BASED APPROACH TO DATA*: LEAVING NO ONE BEHIND IN THE 2030 AGENDA FOR SUSTAINABLE DEVELOPMENT. 2018. Available from: https://www.ohchr.org/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf. Access on: 10 Sep. 2019.

PASSARELLI, Vinícius. LGPD: entenda o que é a Lei Geral de Proteção de Dados Pessoais. *O Estadão*. Online, n.p. 31 May 2019. Available from: https://politica.estadao.com.br/blogs/fausto-macedo/lgpd-entenda-o-que-e-a-lei-geral-de-protecao-de-dados-pessoais/. Access on: 11 Sep. 2019.

RULE, James B.. *Privacy in peril.* Oxford: Oxford University Press, 2007.

SLOOT, B. van Der. Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation. *International Data Privacy Law*, [*S.l.*], v. 4, n.

Revista Direitos Culturais | Santo Ângelo | v. 15 | n. 36 | p. 209-232 | maio/agos. 2020
DOI: http://dx.doi.org/10.20912/rdc.v15i36.18

4, p. 307-325, 3 July 2014. Oxford University Press (OUP). Available from: http://dx.doi.org/10.1093/idpl/ipu014. Access on: 03 Sep. 2019.

SOLOVE, Daniel J.. *The Digital Person:* Technology and Privacy in the Information Age. New York: New York University Press, 2004.

TOVI, Muli David; MUTHAMA, Mutua Nicholas. ADDRESSING THE CHALLENGES OF DATA PROTECTION IN DEVELOPING COUNTRIES. *European Journal of Computer Science and Information Technology*, [*S.l.*], v. 1, n. 2, p.1-9, Sept. 2013.

TZANOU, M.. Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. *International Data Privacy Law*, [*S.l.*], v. 3, n. 2, p. 88-99, 20 Mar. 2013. Oxford University Press (OUP). Available from: http://dx.doi.org/10.1093/idpl/ipt004. Access on: 03 Sep. 2019.

UN. *PERSONAL DATA PROTECTION AND PRIVACY PRINCIPLES*. 2018. Available from: https://www.unsceb.org/CEBPublicFiles/UN-Principles-on-Personal-Data-Protection-Privacy-2018.pdf. Access on: 27 Aug. 2019.

UNCTAD. *Data Protection and Privacy Legislation Worldwide*. 2019. Available from: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx. Access on: 27 Aug. 2019.

UNITED STATES. United States Supreme Court. New York Times Co. V. United States nº 403 U.S. 713. *New York Times Co. v. United States (no. 1873)*. [S.l].