After Brazil's Data Protection Law: Authorizing the Access to Personal Data in Solid

Jefferson O. Silva
silvajo@pucsp.br
Pontifical Catholic University of São Paulo
São Paulo, Brazil

Newton Calegari
newton@nic.br
Brazilian Network Information Center - NIC.br
São Paulo, Brazil

Diogo Cortiz
Inria Paris-Rocquencourt
São Paulo, Brazil

ABSTRACT

Write the abstract here.

CCS CONCEPTS

• **Computer systems organization** → **Embedded systems**; *Redundancy*; Robotics; • **Networks** → Network reliability.

KEYWORDS

Solid, Access control, Decentralized web, Frameworks, Guardian

ACM Reference Format:
Jefferson O. Silva, Newton Calegari, and Diogo Cortiz. 2018. After Brazil's Data Protection Law: Authorizing the Access to Personal Data in Solid. In *Woodstock '18: ACM Symposium on Neural Gaze Detection, June 03–05, 2018, Woodstock, NY*. ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

With the approval of the Brazilian General Data Protection Law (LGPD),[1] several software companies need to redesign the applications they handle the personal data of Brazilian citizens. LGPD is based on the General Data Protection Regulation (GDPR),[2] which aims at protecting the personal data of EU individuals. In total, around 120 countries adopt comprehensive privacy laws and regulations to protect personal data held by private and public bodies [1]. Nevertheless, for the LGPD success, there must be not only fair regulation enforcement but also technological advancements, which potentially includes adopting new software development tools.

Tim Berners-Lee and colleagues propose a platform called Solid (derived from "**So**cial **li**nked **d**ata"), which is can be described as a set of principles, conventions, and tools for building decentralized Web applications [REF]. An application is considered decentralized when it does not hold users' personal data [REF]. LGPD considers personal any data that directly or indirectly leads to the identification of a user [REF]. Solid is based on the principle that users should have full ownership of their personal data. Currently, applications (e.g., Facebook, LinkedIn, Santander) work as "data silos" and all the personal data created in these platforms are controlled by the application companies. In constrast, decentralized Web applications provide complete separation between users' data and the applications that create and consume this data. While users store data in Web-accessible personal online datastores (pods), applications access users data relying as much as possible in W3C standards and Semantic Web technologies [REF]. Pods are independent of applications, which means that the users can change the application that create or consume their personal data at anytime. Users can also grant or restrict access to their pods using Web Access Controls (WAC).

One implication of using Solid in the context of LGPD is that decentralized Web applications need to respond differently according to the citizenship of the user.

We propose

2 BACKGROUND

In this section, we offer some background on LGPD, decentralized Web, and on access control.

2.1 Brazilian Data Protection Law

The LGPD is strong inspired by the European GDPR. The Brazilian Bill, as the European one, defines cross-border jurisdiction, thus the Bill is applicable to any organizations processing personal data of Brazilian residents, whether it is headquartered in Brazil or not.

LGPD has also included the right of data portability, the right of access to personal data by the owner, and the right of erasure. Differently of the GDPR, which imposes 30 days for the controllers to comply with these requests, the LGPD imposes 15 days.

The Brazilian law also requires companies to nominate a Data Protection Officer (DPO) who will be in charge of monitoring the adoption of best practices for personal data protection and for reporting to the National Data Protection Authority (ANPD).

[1] http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm
[2] http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf

LA WEB, June 03–05, 2018, Woodstock, NY

ACM ISBN 978-1-4503-9999-9/18/06…$15.00
https://doi.org/10.1145/1122445.1122456

The regulation defines the concepts of personal data as "any data, isolated or aggregated to another, that may allow the identification of a nutral person or subject them to a certain behavior" [REF] (IAPP: https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/); sensitive data refers to data that may be subject to discriminatory practices, such as political opinion, sexual life, religious belief, genetic and biometric data, and it should have additional security layers; Unless it is possible to reverse-engineering the anonimized data, the law does not apply to this kind of data.

In a technical perspective, the efforts related to the decentralization of the Web help to build systems that are privacy-friendly, respecting user's privacy and in compliance with the regulations. Ainda nao sei se esse paragrafo fica nessa section ou na proxima.

2.2 Decentralized Web

Teste [2]

2.3 Access Control in the Decentralized Web

Access control is typically split into two distinct procedures: authentication, and authorization. While authentication is concerned with determining whether a subject is who it claims to be, authorization is responsible for verifying if the subject is allowed to execute a protected resource. A subject is a term that refers to a user or any other external agent to the system.

3 METHOD

4 PRELIMINARY RESULTS

5 CONCLUSION

ACKNOWLEDGMENTS

To Robert, for the bagels and explaining CMYK and color spaces.

REFERENCES

[1] David Banisar. 2011. Data Protection Laws Around the World Map. *SSRN Electronic Journal* (2011). https://doi.org/10.2139/ssrn.1951416

[2] Axel Polleres, Maulik R Kamdar, Javier David Fernandez Garcia, Tania Tudorache, and Mark A Musen. 2018. A more decentralized vision for linked data. (2018).