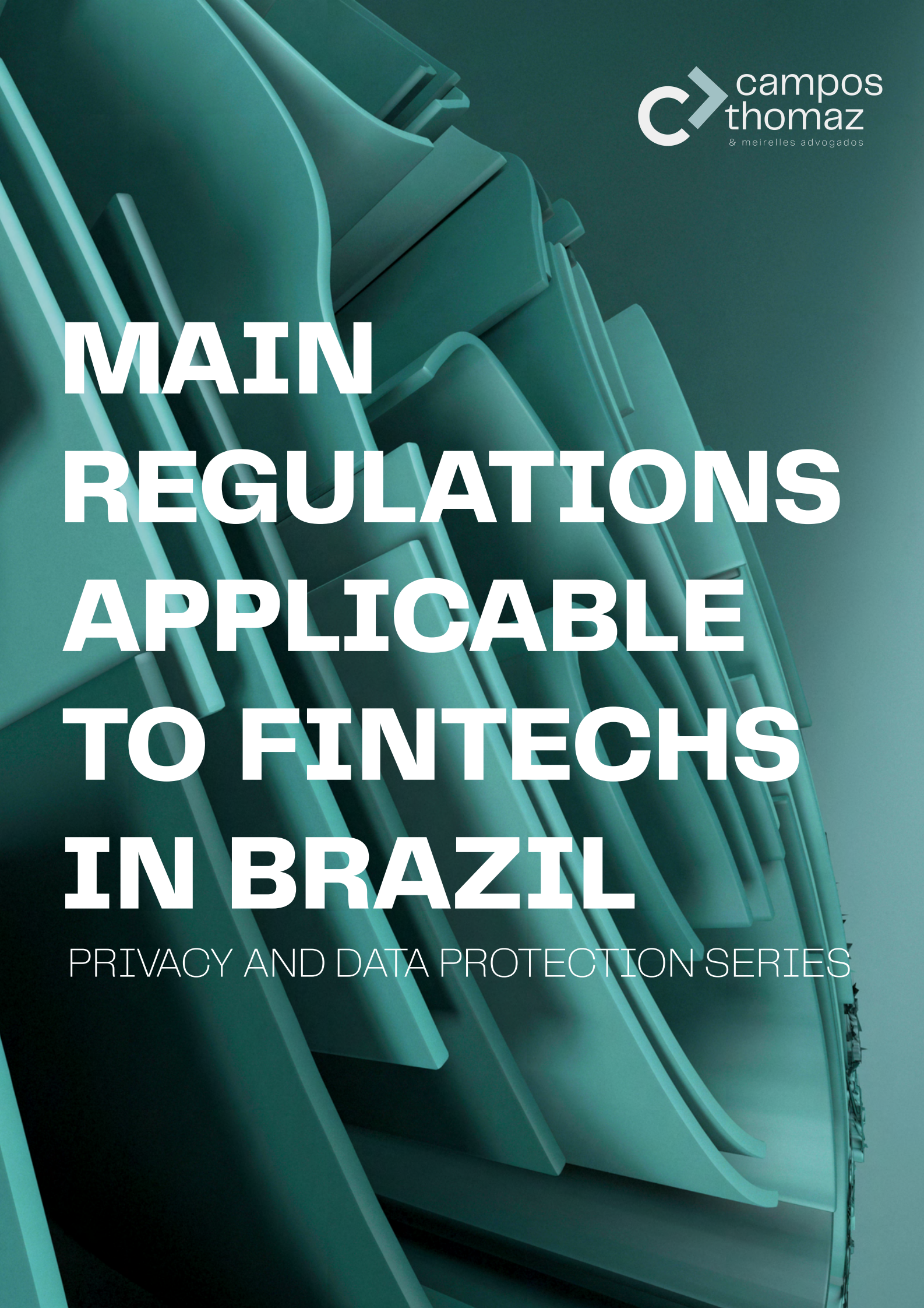

campos thomaz
& meirelles advogados

MAIN REGULATIONS APPLICABLE TO FINTECHS IN BRAZIL

PRIVACY AND DATA PROTECTION SERIES

1. BANK SECRECY

Complementary Law 105/2001[1] ("Bank Secrecy Law") regulates the confidentiality of information and bank data of individuals and legal entities, applying to operations carried out in financial institutions, fintechs, and other companies in the financial market.

The mentioned law lists as non-violation of the duty of secrecy the following hypotheses:

I

The sharing of information between financial institutions for registration purposes.

II

The provision of registration information to credit protection entities.

III

The sharing of financial and payment data to database managers to form credit history, among other situations.

In addition, the Bank Secrecy Law establishes in which specific situations bank secrecy may be breached, for example, in the event of a court order or a request from tax and regulatory authorities, when necessary for investigations of money laundering, tax evasion, or other financial crimes.

[1] Available at: <https://www.planalto.gov.br/ccivil_03/Leis/LCP/Lcp105.htm>. Accessed on: March 16, 2023.

2. GENERAL DATA PROTECTION LAW

Law No. 13,709/2018 ("General Data Protection Law" or, as called in Brazil, "Lei Geral de Proteção de Dados", also known as "LGPD") establishes rules and guidelines for the processing of personal data, both in the virtual and physical environment and in the public and private spheres. Its main objective is to guarantee privacy protection and the fundamental rights of the data subjects[2].

In general terms, the LGPD determines that:

a Data processing agents must keep a record of the personal data processing operations they conduct, especially when based on the legal basis of legitimate interest.

b Controllers must provide a communication channel so that data subjects can exercise their rights under the LGPD.

c Data processing must be carried out according to one of the legal bases provided for in the LGPD.

d The data controller must appoint a Data Protection Officer (also known as "DPO") responsible for mediating communication between the organization, the National Data Protection Authority (as called in Brazil, "Autoridade Nacional de Proteção de Dados", also known as "ANPD"), and data subjects.

e The controller must prepare a Data Protection Impact Assessment – DPIA (as called in Brazil, "Relatório de Impacto à Proteção de Dados Pessoais", also known as "RIPD") to assess the risks involved in the processing of personal data.

f Criteria and procedures used in automated decision-making by the controller must be informed, observing commercial and industrial secrets.

g The ANPD and the data subjects must be communicated in the event of an information security incident involving personal data that may generate risk or relevant damage to the data subjects.

h Technical and administrative security measures must be adopted to protect personal data from unauthorized access and accidental or illicit situations of destruction, loss, alteration, communication, or any form of inadequate or unlawful processing.

[2] Available at: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Accessed on: March 16, 2023.

— 2.1 CD/ANPD Resolution No. 2/2022

CD/ANPD Resolution No. 2/2022[3] approved the regulation for the application of the LGPD, bringing flexibility and more favorable aspects to the development of business for small processing agents, as defined in article 2, item I[4]. Among the flexibilities provided for in the Resolution, small agents can:

Prepare and maintain a record of data processing operations in a simplified format.

Implement a simplified information security policy.

Report data security incidents involving personal data through a simplified procedure and in a doubled timeframe, except when there is a potential compromise of the physical or moral integrity of the data subjects or national security.

Respond to requests from data subjects in a doubled timeframe, among other benefits.

In this sense, fintechs must carry out a diligent and cautious assessment regarding their compliance with the Resolution, given that there are general and specific criteria that determine the non-applicability of the planned flexibility[5].

— 2.2 Cybersecurity

The Resolution of the National Monetary Council (as called in Brazil “Conselho Monetário Nacional”, also known as "CMN") No. 4,893/2021[6] and the Resolution of the Central Bank of Brazil (as called in Brazil "Bacen") No. 85/2021[7] establish guidelines on the cybersecurity policy, action plan, and response to incidents, in addition to requirements for contracting cloud processing and storage services. Such regulations must be observed by fintechs and payment institutions ("PI") authorized to operate by Bacen.

It is worth mentioning that although PIs are considered fintechs, they are not submitted to the rules determined by Resolution No. 4,893/2021. Instead, PIs must follow the provisions outlined in Resolution No. 85/2021 when they receive authorization from BACEN to operate.

3 Available at: < https://in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019>. Accessed on: March 16, 2023.

4 CD/ANPD Resolution No. 2/2022, Art. 2, item I. small-sized processing agents: very small companies, small-sized companies, startups, legal entities governed by private law, including non-profit entities, under the terms of current legislation, as well as natural persons and depersonalized private entities that process personal data, assuming typical controller or processor obligations.

5 Such as the processing of personal data that may significantly affect the interests and fundamental rights of the data subjects (e.g., financial fraud or identity theft) and the processing of personal data in the context of decisions taken solely based on automated processing of personal data, including those intended to define the personal, consumption, and credit profile or aspects of the data subject's personality.

6 Available at: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=RESOLU%C3%87%C3%83O%20CMN&numero=4893>. Accessed on: March 16,

7 Available at: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=85>. Accessed on: March 16, 2023.

3. FRAUD PREVENTION

With the expansion of the digital economy, criminals who operate in the virtual world can exploit the technologies used by fintechs to carry out illicit practices, such as identity theft, money laundering, financial fraud, among others. Therefore, fraud prevention is critical to the industry and must be addressed using appropriate technology.

For fraud prevention, organizations must adopt compliance programs, implement robust compliance and customer assessment processes, risk analysis, continuous monitoring, implementation of cybersecurity policies, and incident response plans. Furthermore, it is also important for organizations to adopt technological measures for information security, such as multi-factor authentication, data encryption, facial recognition technology, and artificial intelligence, among other resources.

However, such resources must always be used in compliance with current legislation, mainly due to the possible risk of discrimination in using certain technologies. For example, artificial intelligence algorithms can be discriminatory in some customer and user reviews.

4. POSITIVE CREDIT REGISTRY

Law No. 12,414/2011 ("Positive Credit Registry Law" or as called in Brazil "Lei do Cadastro Positivo", also known as "LCP")[8] created a register that gathers information on consumer creditworthiness and can be used as a basis for credit analysis, aiming to increase credit availability and reduce interest rates for consumers who have a good payment history.

Fintechs that offer credit analysis services, loans, and other financial services with lower interest rates can use the Positive Credit Registry information to assess their customers' credit risk. However, to use information from the Positive Credit Registry, fintechs must comply with the provisions of the LCP, which establishes rules for using this data.

Among the main provisions of the LCP, it is worth highlighting the need to inform data subjects about the inclusion of their information in the registry, the possibility of contesting the information, and the prohibition of discrimination by companies.

In summary, the LCP is an important tool for risk analysis and credit granting in Brazil. Its applicability to fintechs is relevant, therefore, fintechs that use the information from the Positive Credit Registry must comply with the provisions of the LCP and the LGPD, ensuring the protection of its customer's personal data and avoiding abusive practices in the credit market.

5. OPEN FINANCE

Open Finance is an evolution of the Open Banking concept that expands its scope to encompass financial services beyond banking services, such as foreign exchange, investments, accreditation, insurance, and pensions. This expansion can be explained because, with the user's express authorization, the institutions participating in Open Finance can access the user's history for analysis and offer personalized services.

in view of this, information security is one of the main concerns of the institutions participating in this new system, which is why they must comply with the CMN and Bacen regulations related to information sharing. Such rules include user consent, authentication and confirmation of identity, as well as implementation[9] of standards and operational procedures, cybersecurity rules, and encryption of shared data. Also, partnerships with institutions not authorized to operate by Bacen should be avoided.

Regarding the Open Finance data and information sharing structure, the so-called APIs (Application Programming Interfaces) will be the bridge between institutions participating in Open Finance, allowing the sharing of customer's data. APIs are "key enablers of new business and innovation"[10] in Open Finance. Still, it is important to remember that the technology comes with risks, such as serious privacy breaches, intrusions, and system attacks. Therefore, the security and privacy of customer's data must be a priority for Open Finance participants, who must increasingly invest in cybersecurity.

8 Available at: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>. Accessed on: March 16, 2023.

9 BACEN. Open Finance. Available at: <https://www.bcb.gov.br/estabilidadefinanceira/openfinance >. Accessed on: March 16, 2023.

10 SENSIDIA, PWC. Report on Digital Strategies with APIs in Latin America (online). Available at: https://content.sensedia.com/hubfs/Report_o_estado_das%20APIs_final_v2.pdf>. Accessed on: March 16, 2023.

Our recognitions

Análise Advocacia (2021)

Chambers & Partners Brazil (2021 & 2022)

Leaders League (2021 & 2022)

Transactional Track Record (2021 & 2022)

The Legal 500 (2022)

Meet our Partners

Alan Campos Thomaz

Partner

Technology & Digital Business, Privacy and Data Protection, Fintechs and Intellectual Property

at@camposthomaz.com

+55 11 9 8375.2627 +1 (650) 6436652

Sérgio Meirelles

Partner

Corporate, M&A, Venture Capital and Wealth

sergio@camposthomaz.com

+55 11 9 7551.9865

Filipe Starzynski

Partner

Litigation & Law Enforcement, Civil, Real State, Labor and Family

filipe@camposthomaz.com

+55 11 9 7151.9639

Juliana Sene Ikeda

Partner

Intellectual Property, Technology, Contracts and Life Sciences

juliana@camposthomaz.com

+55 11 9 8644.1613

Follow us

campos thomaz & meirelles advogados

Subscribe to our newsletter