campos thomaz
& meirelles advogados

PRINCIPAIS REGULAÇÕES APLICÁVEIS ÀS FINTECHS NO BRASIL

SÉRIE PRIVACIDADE E PROTEÇÃO DE DADOS

1. SIGILO BANCÁRIO

A Lei Complementar 105/2001[1] ("Lei do Sigilo Bancário") regula a confidencialidade das informações e dados bancários de pessoas físicas e jurídicas, aplicando-se às operações realizadas em instituições financeiras, fintechs e outras sociedades empresárias do mercado financeiro.

Referida lei elenca como não violação ao dever de sigilo as seguintes hipóteses:

I

O compartilhamento de informações entre instituições financeiras para fins cadastrais

II

O fornecimento de informações de cadastro para entidades de proteção ao crédito

III

compartilhamento de dados financeiros e de pagamentos para gestores de banco de dados para formação de histórico de crédito, dentre outras situações, etc.

Além disso, a Lei do Sigilo Bancário estabelece em quais situações específicas que o sigilo bancário pode ser quebrado, como, por exemplo, em caso de ordem judicial ou solicitação de autoridades fiscais e regulatórias; quando necessário para investigações de lavagem de dinheiro, evasão fiscal ou outros crimes financeiros.

[1] Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/LCP/Lcp105.htm>. Acesso em: 16 mar.2023.

2. LEI GERAL DE PROTEÇÃO DE DADOS

A Lei nº 13.709/2018 ("Lei Geral de Proteção de Dados" ou "LGPD") estabelece normas e diretrizes para o tratamento de dados pessoais, tanto no ambiente virtual quanto no físico, em âmbito público e privado. Seu principal objetivo é garantir a proteção da privacidade e dos direitos fundamentais dos titulares dessas informações[2].

Em linhas gerais, a LGPD determina que:

a Os agentes de tratamento devem manter um registro das operações de tratamento de dados pessoais que conduzem, principalmente quando fundamentadas na base legal do legítimo interesse.

b Os controladores devem disponibilizar um canal de comunicação para que os titulares dos dados possam exercer seus direitos previstos na LGPD.

c O tratamento de dados deve ser realizado em consonância com uma das bases legais previstas na LGPD.

d O controlador de dados deve nomear um Encarregado (também conhecido como "Data Protection Officer" ou "DPO"), responsável por intermediar a comunicação entre a organização, a Autoridade Nacional de Dados Pessoais ("ANPD") e os titulares de dados;

e O controlador deve elaborar um Relatório de Impacto à Proteção de Dados Pessoais ("RIPD"), para avaliar os riscos envolvidos no tratamento de dados pessoais.

f Informar os critérios e procedimentos utilizados em tomada de decisões automatizadas pelo controlador, observados os segredos comercial e industrial;

g Realizar comunicação à ANPD e aos titulares de dados em caso de incidente de segurança da informação envolvendo dados pessoais que possa gerar risco ou dano relevante aos titulares; e

h Adotar medidas de segurança, técnicas e administrativas, para proteger os dados pessoais de acessos não autorizados, bem como de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

2 Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 16 mar.2023.

— 2.1 Resolução CD/ANPD nº 2/2022

A Resolução CD/ANPD nº2/2022[3] aprovou o regulamento de aplicação da LGPD, trazendo flexibilizações e aspectos mais favoráveis ao desenvolvimento de negócios para agentes de tratamento de pequeno porte, conforme definição de seu artigo 2º, inc. I[4]. Entre as flexibilizações previstas na Resolução, os agentes de pequeno porte podem:

- Elaborar e manter registro das operações de tratamento de dados em formato simplificado;
- Implementar política de segurança da informação simplificada;
- Comunicar incidentes de segurança da informação envolvendo dados pessoais por meio de procedimento simplificado e em prazo dobrado, salvo quando houver potencial comprometimento à integridade física ou moral dos titulares ou à segurança nacional;
- Responder às solicitações de titulares de dados em prazo dobrado, dentre outros benefícios.

Nesse sentido, é importante que as fintechs realizem uma avaliação diligente e cautelosa quanto ao seu enquadramento na Resolução, tendo em vista que existem critérios gerais e específicos determinantes para a não aplicabilidade das flexibilizações previstas[5].

— 2.2 Segurança Cibernética

A Resolução do Conselho Monetário Nacional ("CMN") nº 4.893/2021[6] e a Resolução do Banco Central do Brasil ("Bacen") nº 85/2021[7] estabelecem diretrizes sobre a política de segurança cibernética, plano de ação e resposta a incidentes, além de requisitos para a contratação de serviços de processamento e armazenamento em nuvem. Tais normativas devem ser observados por fintechs e instituições de pagamento ("IP") autorizadas a funcionar pelo Bacen.

Vale mencionar que, apesar das IP serem consideradas fintechs, elas não estão sujeitas às regras determinadas pela Resolução nº 4.893/2021. Em vez disso, as IPs devem seguir as disposições previstas na Resolução nº 85/2021, quando receberem autorização do BACEN para funcionamento.

3 Disponível em: < https://in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019>. Acesso em: 16 mar.2023.

4 Resolução CD/ANPD nº2/2022, Art. 2º, inc. I. agentes de tratamento de pequeno porte: microempresas, empresas de pequeno porte, startups, pessoas jurídicas de direito privado, inclusive sem fins lucrativos, nos termos da legislação vigente, bem como pessoas naturais e entes privados despersonalizados que realizam tratamento de dados pessoais, assumindo obrigações típicas de controlador ou de operador.

5 Como o tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares (e.g., fraudes financeiras ou roubo de identidade) e o tratamento de dados pessoais no contexto de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, inclusive aquelas destinadas a definir o perfil pessoal, de consumo e de crédito ou os aspectos da personalidade do titular.

6 Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=RESOLU%C3%87%C3%83O%20CMN&numero=4893>. Acesso em: 16 mar.2023.

7 Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=85>. Acesso em: 16 mar.2023.

3. PREVENÇÃO À FRAUDE

Com a expansão da economia digital, criminosos que operam no mundo virtual podem explorar as tecnologias utilizadas pelas fintechs para realizar práticas ilícitas, tais como roubo de identidade, lavagem de dinheiro, fraude financeira, entre outras. Desse modo, a prevenção à fraude é fundamental para o setor e deve ser abordada por meio do uso de tecnologia adequada.

Para prevenção à fraude, é crucial que as organizações adotem programas de compliance, implementando processos robustos de conformidade e de avaliação de clientes, análise de riscos, monitoramento contínuo, implementação de políticas de segurança cibernética e planos de resposta a incidentes. Além disso, é importante que as organizações adotem também medidas tecnológicas de segurança da informação, tais como autenticação multifatorial, criptografia de dados, tecnologia de reconhecimento facial, inteligência artificial, entre outros recursos.

Todavia, é importante que tais recursos sejam utilizados sempre em conformidade com a legislação vigente, principalmente devido ao possível risco discriminatório no uso de certas tecnologias. Por exemplo, algoritmos de inteligência artificial podem ser discriminatórios em algumas análises de clientes e usuários.

4. CADASTRO POSITIVO

A Lei nº 12.414/2011 ("Lei do Cadastro Positivo" ou "LCP")[8] criou um cadastro que reúne informações de adimplência dos consumidores e pode ser utilizado como base para análise de crédito, tendo como objetivo aumentar a oferta de crédito e reduzir os juros para os consumidores que possuem bom histórico de pagamentos.

As fintechs que oferecem serviços de análise de crédito, empréstimos e outros serviços financeiros com juros mais baixos podem utilizar as informações do Cadastro Positivo para avaliar o risco de crédito de seus clientes. No entanto, para utilizar as informações do Cadastro Positivo, as fintechs devem cumprir com as disposições da LCP, que estabelece regras para a utilização desses dados.

Entre as principais disposições da LCP, destaca-se a necessidade de informar aos titulares dos dados sobre a inclusão de suas informações no cadastro, a possibilidade de contestação das informações e a proibição de discriminação por parte das empresas.

Em resumo, a LCP é uma importante ferramenta para a análise de risco e concessão de crédito no Brasil, e sua aplicabilidade às fintechs é relevante, de modo que as fintechs que utilizam as informações do Cadastro Positivo devem cumprir com as disposições da LCP e da LGPD, garantindo a proteção dos dados pessoais de seus clientes e evitando práticas abusivas no mercado de crédito.

5. OPEN FINANCE

O Open Finance é uma evolução do conceito de Open Banking, na medida em que expande o seu escopo para abranger serviços financeiros, além dos serviços bancários, como câmbio, investimentos, credenciamento, seguros e previdência. Isso porque, mediante a autorização expressa do usuário, as instituições participantes do Open Finance podem acessar o histórico do usuário para análise e oferta de serviços personalizados.

À vista disso, a segurança da informação é uma das principais preocupações das instituições participantes deste novo sistema, de modo que estas devem cumprir com as regras do CMN e Bacen relacionadas ao compartilhamento das informações. Isso inclui o consentimento do usuário, autenticação e confirmação de identidade, além de implementação de[9] padrões e procedimentos operacionais, regras de segurança cibernética e criptografia de dados compartilhados. Ainda, parcerias com instituições não autorizadas a funcionar pelo Bacen devem ser evitadas.

Em relação à estrutura de compartilhamento de dados e informações do Open Finance, as denominadas APIs (Application Programing Interfaces) serão a ponte entre as instituições participantes do Open Finance, permitindo o compartilhamento de dados de clientes. As APIs são como "habilitadoras-chave de novos negócios e inovação"[10] no Open Finance, mas é importante lembrar que a tecnologia também apresenta riscos, como violações graves de privacidade, invasões e ataques em sistemas. Portanto, a segurança e a privacidade dos dados dos clientes devem ser priorizadas pelos participantes do Open Finance, que devem investir cada vez mais em cibersegurança.

8 Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>. Acesso em: 16 mar.2023.

9 BACEN. Open Finance. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/openfinance >. Acesso em 16 mar.2023.

10 SENSIDIA, PWC. Report sobre Estratégias Digitais com APIs na América Latina (online). Disponível em: <https://content.sensedia.com/hubfs/Report_o_estado_das%20APIs_final_v2.pdf>. Acesso em: 16 mar.2023.

Nossos reconhecimentos

Análise Advocacia (2021)

Chambers & Partners Brazil (2021 e 2022)

Leaders League (2021 e 2022)

Transactional Track Record (2021 e 2022)

The Legal 500 (2022)

Conheça nossos Sócios

Alan Campos Thomaz

Sócio

Tecnologia e Negócios Digitais, Privacidade e Proteção de Dados, Fintechs e Propriedade Intelectual

at@camposthomaz.com

+55 11 9 8375.2627 +1 (650) 6436652

Sérgio Meirelles

Sócio

Societário, M&A, Venture Capital e Wealth

sergio@camposthomaz.com

+55 11 9 7551.9865

Filipe Starzynski

Sócio

Contencioso & Law Enforcement, Consultivo Cível, Imobiliário, Trabalhista e Família

filipe@camposthomaz.com

+55 11 9 7151.9639

Juliana Sene Ikeda

Sócia

Propriedade Intelectual, Tecnologia, Contratos e Life Sciences

juliana@camposthomaz.com

+55 11 9 8644.1613

Nos acompanhe em nossas redes

campos thomaz & meirelles advogados

Assine nossa newsletter