RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

OPEN BANKING: EVOLUÇÃO OU VIOLAÇÃO A LGPD

OPEN BANKING: EVOLUTION OR VIOLATION THE LGPD

Jonathas Alves Mesquita [45]
José Elias Seibert Santana Junior [46]
Submetido em: 16/05/2022
Aprovado em: 16/05/2022
Publicado em: 16/05/2022 v. 2, n. 1, jan-jun. 2022
DOI: 10.51473/rcmos.v2i1.295

RESUMO
Este artigo buscou apresentar sobre o Open Banking e a Lei Geral de Proteção de Dados (LGPD). O Open Banking é um sistema que permite que o banco compartilhe as informações de seus clientes a fim de sugerir melhorias e planos diferentes para ele. Com isso, este estudo teve por objetivo geral dissertar sobre a evolução ou violação da LGPD no âmbito do Open Banking. A metodologia utilizada foi a revisão de literatura, onde consultou-se diferentes bancos de dados (nacionais e internacionais) a fim de analisar os documentos científicos disponíveis acerca dessa temática, coletando informações e compilando as mesmas. Dessa forma, conclui-se a importância de autorizar ou não o Banco de compartilhar os dados, a fim de proteger as informações pessoais.

Palavras-chave: Open Banking. Lei Geral de Proteção de Dados. LGPD.

ABSTRACT
This article sought to present about Open Banking and the General Data Protection Law (LGPD). Open Banking is a system that allows the bank to share its customers' information to suggest improvements and different plans for the same. Thus, this study aimed to discuss the evolution or violation of LGPD in the context of Open Banking. The methodology used was the literature review, where different databases (national and international) were consulted to analyze the scientific documents available on this subject, collecting information and compiling them. Thus, it is concluded the importance of authorizing or not the Bank to share data, to protect personal information.
Keywords: Open Banking. General Data Protection Act. GDPR

1 INTRODUÇÃO

Este estudo procurou desenvolver a temática "Open Banking: Evolução ou Violação a LGPD". Com a tecnologia evoluindo cada vez mais e os procedimentos bancários sendo digitalizados, a Lei Geral de Proteção de Dados (LGPD) visa que qualquer informação a respeito do cliente deve ser mantida em sigilo a menos que o cliente solicite que seus dados sejam compartilhados.
Como hipótese teremos:
a) O banco deve manter os dados dos clientes em sigilo absoluto, não compartilhando os mesmos;
b) Ao contratar um banco, o cliente deve ficar ciente a respeito da política de preservação de dados;
c) O cliente deve expor para seu gerente que seus dados fiquem sob sigilo absoluto, podendo ser compartilhados apenas mediante autorização prévia.
Este estudo apresentou a seguinte problemática: Como a LGPD evoluiu ou violou o open banking?
Por objetivo geral temos: Dissertar sobre a evolução ou violação da LGPD no âmbito do Open Banking e por objetivos específicos: a) Conceituar a LGPD (Lei Geral de Proteção de Dados); b) Discorrer sobre o open banking: suas funcionalidades, benefícios, aplicações e c) Explanar sobre como a LGPD evoluiu ou violou o open banking.
Com o acesso cada vez mais frequente à internet, os bancos se modernizaram e com isso surgiu o open banking que deve estar em concordância com a LGPD afim de garantir a segurança de seus usuários.
Assim, este estudo se justifica trazendo importantes implicações para a sociedade e estudiosos da área, servindo ainda como apoio acadêmico para pesquisas futuras.

2 METODOLOGIA

45
46 [1] Graduando em Direito pela Faculdade Santo Agostinho – FASAVIC (ALUNO)
Advogado. Professor de Direito do Trabalho, atualmente coordenador do curso de Direito da FASAVIC. Especialista em Direito do Trabalho e Direito Processual do Trabalho pela faculdade Damásio de Jesus. (ORIENTADOR)

Para que este estudo seja desenvolvido será adotado o método descritivo, com abordagem qualitativa. Shank (2002 p. 5) define a pesquisa qualitativa como "uma forma de investigação empírica sistemática sobre o significado".
Por sistemática, ele significa "planejado, ordenado e público", seguindo as regras acordadas pelos membros da comunidade de pesquisa qualitativa. Por empírico, ele quer dizer que esse tipo de investigação está fundamentado no mundo da experiência.
A investigação sobre o significado diz que os pesquisadores tentam entender como os outros dão sentido à sua experiência.
Denzin e Lincoln (2000 p. 3) afirmam que a pesquisa qualitativa envolve uma abordagem interpretativa e naturalista: "Isso significa que os pesquisadores qualitativos estudam as coisas em seus ambientes naturais, tentando compreender ou interpretar fenômenos em termos dos significados que as pessoas trazem para eles".
O estudo foi elaborado por meio de pesquisa de revisão bibliográfica. Para Marconi e Lakatos (2010), uma revisão de literatura é uma análise crítica de fontes publicadas, ou literatura, sobre um tópico específico.
É uma avaliação da literatura e fornece um resumo, classificação, comparação e avaliação. No nível de pós-graduação, as revisões da literatura podem ser incorporadas em um artigo, um relatório de pesquisa ou uma tese.
Em nível de graduação, as revisões de literatura podem ser uma avaliação autônoma separada.
Para Köche (2011), a revisão da literatura é geralmente no formato de um ensaio padrão composto de três componentes: uma introdução, um corpo e uma conclusão. Não é uma lista como uma bibliografia anotada na qual um resumo de cada fonte é listado um por um.
A busca será realizada em bases de dados da Literatura Latino-Americana e do Caribe em Ciências da Saúde (LILACS), Scientific Electronic Library Online (SCIELO), monografias, dissertações, artigos científicos.
Os critérios de inclusão para o levantamento bibliográfico deste estudo serão texto disponíveis na íntegra de maneira gratuita, nas línguas portuguesa e inglesa e que atendam aos objetivos propostos. Os critérios de exclusão serão estudos que não atendam os objetivos do estudo.

3 CONCEITO DE OPEN BANKING

O cliente é o proprietário de seus dados, não o banco. Essa é a proposta do Open Bank, que é responsável por tornar o usuário o protagonista do controle e permitir que as instituições financeiras acessem suas informações pessoais. O modelo de banco aberto visa ampliar a oferta de produtos e serviços bancários a um custo menor. No entanto, o grande desafio será criar métodos apropriados para coletar e gerenciar o consentimento para o processamento de dados pessoais (GOETTENAUER, 2020).
O open banking é uma forma de expandir os produtos e serviços bancários a um custo menor, criando uma competição mais saudável entre os bancos e a tecnologia financeira. No entanto, neste caso, tendo em conta a Lei Geral de Proteção de Dados (LGPD), o maior desafio será criar um processo adequado para recolher e gerir o consentimento do cliente para participar neste novo modelo e o tratamento de dados pessoais (BARBERIS; BUCKLEY; ARNER, 2015).
No modelo estipulado pelo Banco Central, as instituições financeiras são classificadas como S1, que é igual ou superior a 10% do Produto Interno Bruto (PIB) ou instituições financeiras com atividades internacionais relacionadas, e S2, que tem uma escala entre os duas das instituições que participam de banco aberto exigem 1% e 10% do PIB (BARBERIS; BUCKLEY; ARNER, 2015).
Portanto, desde que os clientes autorizem o compartilhamento de dados, os grandes bancos que operam no Brasil serão obrigados a participar. Por outro lado, outras instituições, como empresas de pagamento e empresas de fintech, terão participação voluntária e devem compartilhar dados de clientes com concorrentes (MAGNUSON, 2017).
Esta situação conduz à abordagem básica do open banking: reciprocidade, tendo em conta que todas as empresas participantes têm o direito de receber dados dos concorrentes e são obrigadas a partilhá-los, desde que o cliente concorde. Assim, a livre concorrência expande e beneficia o mais interessado, nomeadamente os consumidores, que terão a opção de partilhar os dados, que será digital e conduzida em ambiente seguro e supervisionado pelos reguladores do Banco Central. O processo obedecerá à Lei Geral de Proteção de Dados (LGPD) e seguirá um processo padrão acordado pelos clientes, semelhante ao acesso a instituições por meio de aplicativos ou banco on-line por meio de reconhecimento facial, biometria ou senhas (VIOLA; HERINGER, 2020).

Como o Open Banking é baseado no consentimento, que é um dos fundamentos legais da LGPD, os clientes podem autorizar ou revogar o compartilhamento a qualquer momento. Vale ressaltar que essa aceitação é específica, ou seja, os clientes só permitem que determinados dados sejam compartilhados com bancos terceirizados, não sendo universalmente aplicável a todos os dados ou a todas as instituições.
A internet ou rede é conhecida como o meio de comunicação mais poderoso do mundo, ela é capaz de nos conectar a qualquer informação desejada em cerca de um instante. No entanto, a Internet como a conhecemos hoje foi projetada para comunicações militares na década de 1960, quando um sistema de compartilhamento de informações foi criado para facilitar a estratégia de guerra.

Assim, o marco inicial da Internet foi chamado de ARPANET, um sistema em que as informações eram quebradas em pequenos pacotes contendo pedaços de dados e, em caso de ataque, era difícil para um adversário obter todas as informações desejadas. Não foi até a década de 1990 que surgiu o famoso "boom da Internet", com o advento do www (World Wide Web) e outros navegadores, popularizando o uso da Internet como uma rede global de computadores conectados.

Não é diferente no Brasil, onde a internet deu seus primeiros passos nos anos 90 e se estabilizou como forma de comunicação nos anos 2000. Com o desenvolvimento da Internet, as formas de busca se expandiram, a informação tornou-se mais acessível aos usuários, a Internet tornou-se uma verdadeira aliada na disseminação da informação, a conveniência da tecnologia trouxe a reconfiguração, ou seja, criou-se uma maneira de distribuir informações e dados.

Assim, confirma-se que surgiram novos questionamentos sobre privacidade e facilidade de movimentação de dados pessoais, e a necessidade de tutela tornou-se mais clara. Em 2014, o Brasil aprovou uma lei que regulamenta a disciplina na Internet, o Marco Civil da Internet, para manter os usuários da Internet seguros.

No entanto, esta nova lei não garante a privacidade de dados de forma completa, abrangente e estruturada, e não é uma disposição geral de proteção de dados, concluindo que a proteção de dados pessoais permanece desprotegida e é necessária legislação que garanta o respeito à privacidade. Fluxo comunitário de dados pessoais.

A LGPD (Lei Geral de Proteção de Dados) está definida na Lei 13.709/18, que dispõe sobre o tratamento de dados pessoais, inclusive meios digitais, por pessoas físicas ou jurídicas de direito público ou privado para a proteção da liberdade e do direito fundamental à privacidade e o livre desenvolvimento da personalidade das pessoas físicas (BRASIL, 2018).

4 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E SUAS PARTICULARES

Em Wheaton v. Peters, 1834, mas não era oficialmente conhecido até 1890, o artigo de Louis Brandeis e Samuel Warren "The Right to Privacy" tratou de uma compilação de decisões dos EUA mostrando que as preocupações com a privacidade são uma ofensa grave às violações de privacidade. seja humano.

No final do século 20, os avanços na tecnologia da computação e no processamento automatizado de dados começaram a tomar forma, então novas legislações começaram a surgir e chamar a atenção. "Por volta de 1970, viu-se que as decisões legais e a legislação reconheciam que os dados pessoais eram uma projeção da personalidade de um indivíduo e, portanto, passíveis de proteção legal (LUGATI; ALMEIDA, 2021).

Na década de 1980, novas leis de proteção de dados foram implementadas na França, Noruega, Suécia e Áustria. Foi nesta altura que em 1981 a Comissão Europeia harmonizou as regras para o tratamento automático de proteção de dados e o livre fluxo desses dados, resultando na Diretiva Europeia de Dados Pessoais, e em 2016 um novo Regulamento (UE) 2016/679, Regulamento Geral de Proteção de Dados.

Hoje no Brasil existe um diploma legal que trata da proteção de dados, a LGPD, mas antes dela entrar em vigor, mesmo que por omissão, a proteção de dados passou a ser tratada pelo artigo 5º X da Constituição Federal, garantindo a privacidade e privacidade. à constituição, outro Esse conceito de proteção também foi iniciado por leis esparsas, como o Código de Defesa do Consumidor quando se trata de proteger os dados do titular de bancos de dados e habeas corpus data, ver orientação de Danilo Doneda sobre o assunto:

> A proteção de dados pessoais no ordenamento brasileiro não se estrutura a partir de um complexo normativo unitário. A Constituição Brasileira contempla o problema da informação inicialmente por meio das garantias à liberdade de expressão e do direito à informação, que deverão eventualmente ser confrontados com a proteção da personalidade e, em especial, com o direito à privacidade. Além disso, a Constituição considera invioláveis a vida privada e a intimidade (art. 5º, X), veja-se especificamente a interceptação de comunicações telefônicas, telegráficas ou de dados (artigo 5º, XII), bem como instituiu a ação de habeas data (art. 5º, LXXII), que basicamente estabelece uma modalidade de direito de acesso e retificação dos dados pessoais. Na legislação infraconstitucional, destaque-se o Código de Defesa do Consumidor, Lei 8.078/90, cujo artigo 43 estabelece uma série de direitos e garantias para o consumidor em relação às suas informações pessoais presentes em "bancos de dados e cadastros", implementando uma sistemática baseada nos Fair Information Principles à matéria de concessão de crédito e possibilitando que parte da doutrina verifique neste texto legal o marco normativo dos princípios de proteção de dados pessoais no direito brasileiro. (DONEDA, 2021)

Em suma, a proteção de dados é uma novidade no Brasil, porém, conforme explicado, é um assunto que vem sendo tratado há décadas, principalmente na Europa, em busca da proteção da vida privada e dos direitos íntimos. As mudanças na privacidade, o aumento da capacidade de coletar, processar e usar informações mudaram o mundo, e as preocupações com quantidades descontroladas de informações criaram algumas leis e um maior respeito à privacidade na sociedade.

A premissa da Lei nº 13.709/2018, que regulamenta o tratamento de dados pessoais no Brasil, é garantir o respeito à vida privada no fluxo comunitário de dados pessoais. Conforme mencionado, seu objetivo é proteger "os direitos fundamentais

de liberdade e privacidade e o livre desenvolvimento da personalidade das pessoas físicas". (BRASIL, 2018), inclui mídia digital, não exclui o ambiente físico, como dados em documentos, currículos, formulários e folha de pagamento. No artigo 2º, a lei define seus fundamentos, a saber: privacidade, autodeterminação da informação; liberdade de expressão, informação, comunicação e opinião; inviolabilidade da intimidade, honra e imagem; desenvolvimento econômico e tecnológico e inovação; livre iniciativa; livre concorrência. e defesa do consumidor; direitos humanos; o livre desenvolvimento da personalidade; a dignidade da pessoa natural e o exercício da cidadania.

O titular dos dados pessoais é a pessoa física (pessoa física) a quem os dados pessoais são processados, deve-se notar aqui que não estão incluídas as pessoas jurídicas, e o artigo 5º da LGPD também define o que são dados pessoais, ou seja, "relacionados pessoa física identificada ou identificável" (BRASIL, 2018) e dados sensíveis, ou seja, "dados pessoais relativos à raça ou etnia, crenças religiosas, opiniões políticas, filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados relacionados ou vida sexual, dados genéticos ou biométricos, quando relacionados a pessoas físicas" (BRASIL, 2018). Além disso, o conceito de terapia precisa ser entendido. reivindicações da LGPD:

> Artigo 5° - X - Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (BRASIL,2018).

Por fim, os princípios orientadores da Lei estão contidos em seu artigo 6º, que, salvo por boa vontade, descreve o princípio da finalidade como "tratamento lícito, específico, claro e informado do titular dos dados, nenhum tratamento incompatível com essas finalidades. possibilidade" (BRASIL, 2018), o princípio da adequação, "compatibilidade do tratamento com a finalidade para a qual o titular dos dados foi informado, dependendo do contexto do tratamento" (BRASIL, 2018), ou seja, que os dados devem ser suficientes, relevantes e relevantes ao seu propósito Não importa.

Existem também os princípios da necessidade, descritos como "restringindo o tratamento ao mínimo necessário para atingir os seus fins, sendo a cobertura dos dados relevantes proporcional à finalidade do tratamento de dados e não excessiva"; o princípio do livre acesso, descrito como "restringindo tratamento à Garantia, consulta facilitada e gratuita sobre a forma e duração do tratamento e a integridade dos seus dados pessoais"; os princípios de qualidade dos dados, descritos como "garantia aos titulares dos dados da exatidão, clareza, relevância e atualidade de seus dados, conforme necessário e cumprindo a finalidade de seu processamento" (BRASIL, 2018), em que o princípio explica que informações incorretas devem ser corrigidas, informações desatualizadas ou irrelevantes devem ser proibidas, ou pode-se solicitar o acréscimo de quaisquer dados para manter a veracidade das informações, com base nisso, é possível fornecer os melhores direitos reservados pelo titular..

Existem ainda os princípios da transparência, que conferem aos titulares o direito à existência de ficheiros de dados; e as medidas de gestão"; o princípio da precaução, que se traduz por "medidas para evitar danos resultantes do tratamento de dados pessoais"; o princípio da não discriminação, que inclui "o tratamento não é possível para fins discriminatórios ilícitos ou abusivos", os dados devem ser tratados para determinados fins, esses fins devem ser comunicados ao titular dos dados. (BRASIL, 2018)

Por fim, o princípio da responsabilidade é reconhecido na lei como "a prova do agente de que foram tomadas medidas efetivas que possam demonstrar o cumprimento das regras de proteção de dados pessoais, e até mesmo a eficácia dessas medidas". (BRASIL, 2018). Por fim, um olhar sobre a importância da nova lei para nossa ordem nacional:

> Estão se tornando os novos insumos da nova economia, o que pode comprometer não apenas a privacidade dos usuários, mas também a identidade pessoal, a autodeterminação informativa, a liberdade, as oportunidades e perspectivas do presente e do futuro das pessoas e a própria democracia. (FRAZÃO, 2021)

E assim, a Lei Geral de Proteção de Dados entrou em nosso ordenamento jurídico, trazendo muitas novidades sobre proteção de dados pessoais e mudando drasticamente a forma como as empresas e órgãos públicos tratam a privacidade e a segurança dos dados dos usuários que terão o direito à informação adequada.

5 LGPD E OPEN BANKING: EVOLUÇÃO OU VIOLAÇÃO?

O consentimento é uma declaração gratuita e óbvia por parte do titular dos dados pessoais de que os seus dados são tratados para uma finalidade específica. De acordo com a LGPD, consentimento é "a expressão livre, informada e inequívoca do consentimento do titular para o tratamento de seus dados pessoais para uma finalidade específica" (Brasil, 2020).

A liberdade de expressão refere-se à escolha do titular de não ser imposto ou vinculado; a expressão informada refere-se à escolha do titular dos dados em consentir um tratamento baseado em informações claras, o conceito de expressão clara

envolve uma ação positiva por parte do titular dos dados, o que não deixa dúvidas de que eles pretendem consentir com o processamento de seus dados pessoais.

Portanto, é direito do titular, deve ser dada a ele a liberdade de escolher o que fazer com seus dados, e essa escolha deve ser articulada para uma finalidade específica e informada. Os requisitos da LGPD visam garantir aos titulares de dados o direito de escolher como seus dados serão processados e de cumprir os princípios fundamentais estabelecidos na LGPD, em especial no que diz respeito à autodeterminação informacional, à proteção do consumidor, à dignidade e ao exercício da cidadania como uma pessoa física.

De acordo com a LGPD, caso o controlador precise compartilhar dados pessoais após obter o consentimento do titular dos dados, deverá informar previamente o titular dos dados sobre o novo método de processamento e obter seu consentimento para essa nova finalidade. Além disso, é importante observar que o ônus da prova em relação à coleta do consentimento caberá ao responsável pelo tratamento dos dados pessoais, e que o processamento dos dados no contexto do vício do consentimento é proibido pela LGPD.

Além do direito de expressar ou não o consentimento, os titulares dos dados também têm outros direitos previstos nos textos legais. Dentre eles, uma lista de direitos é mencionada no Capítulo III da LGPD, direitos esses que derivam dos princípios de liberdade, intimidade e privacidade.

De acordo com o texto, o titular tem o direito de confirmar e aceder aos seus dados e solicitar a correção caso os dados estejam incompletos, imprecisos ou desatualizados, garantindo assim a sua qualidade; informação sobre a possibilidade de não dar o seu consentimento e retirada do consentimento pode ser solicitado.

Além disso, a LGPD permite que os titulares transfiram seus dados para outro provedor de serviço ou produto, direito que se confunde pontualmente com um dos objetivos do Open Banking. Além de proteger o controle dos titulares sobre seus dados, a maioria dos direitos dos titulares estabelecidos na LGPD possibilitam ajustar e melhorar a oferta de produtos e serviços às pessoas físicas, por exemplo, o tratamento de dados completos, e atualização, otimização do mercado de crédito e base do funcionamento orgânico, afetando diretamente os mercados financeiros e outros setores da economia.

Quais são as situações em que os indivíduos são obrigados a transferir dados para o banco? Além da legislação em todo o Brasil, o setor financeiro está sujeito a diversas regulamentações setoriais. As transferências de dados financeiros de pessoas físicas para instituições financeiras podem ocorrer entre instituições financeiras e consumidores, bem como entre as próprias instituições financeiras.

A relação de troca de dados entre consumidores e instituições financeiras é projetada para servir ao propósito de prestação de serviços financeiros, mas também pode apoiar as instituições financeiras no cumprimento de suas obrigações perante autoridades e reguladores. Em alguns casos, as instituições financeiras processam e compartilham dados de consumidores devido à necessidade de envio de informações sobre atividades ilegais ou abusivas, de acordo com os termos das leis e regulamentos vigentes, de acordo com o Artigo 7º(II) e Artigo 11(II) da LGPD.

Essas ações podem ser oferecidas aos órgãos reguladores do setor, Banco Central do Brasil (BCB), Comissão de Valores Mobiliários (CVM) e Comissão de Controle de Atividades Financeiras (COAF). De acordo com a Lei nº 9.613/1998, existem ações que podem fornecer indícios de crimes contra o sistema financeiro do país, como exemplos de situações que levam à notificação compulsória e, portanto, ao compartilhamento de dados pessoais por instituições financeiras.

Além disso, é legal que as instituições financeiras troquem informações relativas ao consumidor com outras instituições financeiras para a formação de bancos de dados, inclusive aqueles relacionados à inadimplência, caso em que a lei de defesa do consumidor está em seu art. O artigo 43.º estabelece a necessidade de transparência e o direito de acesso e retificação do consumidor, e impõe requisitos à sua legalidade.

Nesse sentido, a Lei do Registro Ativo (12.414/2011) regulamenta a formação e as obrigações em relação às bases de dados de histórico de crédito, alterada pela Lei Complementar 166/2019. As mudanças ampliaram o acesso aos dados do consumidor e estabeleceram a possibilidade de incluir automaticamente os dados do consumidor (opt-in) e excluí-los mediante solicitação (opt-out).

Aqui, verifica-se uma contradição com a LGPD sobre o consentimento, mas a LGPD fornece uma base legal para proteção de crédito para justificar tais operações de processamento de dados. Dessa forma, qualquer conflito de leis pode precisar ser resolvido pela autoridade judiciária competente. Além disso, as diretrizes da ANPD ajudam a equilibrar a base legal para consentimento e proteção ao crédito. Ressalta-se que a troca de informações realizada pelas instituições financeiras deve obedecer aos requisitos de sigilo bancário, bem como aos estabelecidos pelo Banco Central do Brasil e pela Comissão de Valores Mobiliários, respeitadas as exceções previstas no art. Artigo 1º da Lei nº 105/2001.

A LGPD apenas conceitua dados pessoais e dados sensíveis, e não especifica dados financeiros ao longo do texto que, ao contrário do que muitos pensam, não se enquadram diretamente na categoria de dados sensíveis. Muitas vezes, os dados financeiros não são dados confidenciais em si, mas dependendo do contexto e de como se relacionam com outros dados pessoais, esses dados podem facilmente se tornar dados confidenciais.

Por exemplo, dados de transações de crédito pessoal que indiquem a compra de medicamentos ou o pagamento de uma consulta podem ser considerados sensíveis porque se referem à saúde do indivíduo. O contexto em que os controladores de dados financeiros analisam quais dados serão considerados dados sensíveis é muito importante, pois regras mais rígidas serão aplicadas ao processamento desses dados sob a LGPD.

Antes da LGPD, os dados financeiros já eram protegidos. A Lei do Sigilo Bancário de 2011 (BRASIL, 2001) e regulamentações do BCB, como a Resolução Conjunta do BCB nº, relativa a sigilo, confidencialidade e proteção de dados. Considerando que não há definição específica do termo "dados financeiros pessoais" na legislação, o conceito será construído com base na Lei do Sigilo Bancário, que prevê em seu § 1º que o sigilo das operações ativas e passivas deve ser protegido • Instituições financeiras e seus serviços.

Portanto, levando em consideração os motivos apresentados, para fins deste relatório, tratamos dados financeiros pessoais como qualquer informação sobre uma pessoa física identificada ou identificável (conforme orientação da LGPD) em relação a transações financeiras ativas e passivas, e serviços prestados.

Essas ações podem ser oferecidas aos órgãos reguladores do setor, Banco Central do Brasil (BCB), Comissão de Valores Mobiliários (CVM) e Comissão de Controle de Atividades Financeiras (COAF). De acordo com a Lei nº 9.613/1998, existem ações que podem fornecer indícios de crimes contra o sistema financeiro do país, como exemplos de situações que levam à notificação compulsória e, portanto, ao compartilhamento de dados pessoais por instituições financeiras.

Além disso, é legal que as instituições financeiras troquem informações relativas ao consumidor com outras instituições financeiras para a formação de bancos de dados, inclusive aqueles relacionados à inadimplência, caso em que a lei de defesa do consumidor está em seu art. O artigo 43.º estabelece a necessidade de transparência e o direito de acesso e retificação do consumidor, e impõe requisitos à sua legalidade.

Nesse sentido, a Lei do Registro Ativo (12.414/2011) regulamenta a formação e as obrigações em relação às bases de dados de histórico de crédito, alterada pela Lei Complementar 166/2019. As mudanças ampliaram o acesso aos dados do consumidor e estabeleceram a possibilidade de incluir automaticamente os dados do consumidor (opt-in) e excluí-los mediante solicitação (opt-out).

Aqui, verifica-se uma contradição com a LGPD sobre o consentimento, mas a LGPD fornece uma base legal para proteção de crédito para justificar tais operações de processamento de dados. Dessa forma, qualquer conflito de leis pode precisar ser resolvido pela autoridade judiciária competente. Além disso, as diretrizes da ANPD ajudam a equilibrar a base legal para consentimento e proteção ao crédito. Ressalta-se que a troca de informações realizada pelas instituições financeiras deve obedecer aos requisitos de sigilo bancário, bem como aos estabelecidos pelo Banco Central do Brasil e pela Comissão de Valores Mobiliários, respeitadas as exceções previstas no art. Artigo 1º da Lei nº 105/2001.

A LGPD apenas conceitua dados pessoais e dados sensíveis, e não especifica dados financeiros ao longo do texto que, ao contrário do que muitos pensam, não se enquadram diretamente na categoria de dados sensíveis. Muitas vezes, os dados financeiros não são dados confidenciais em si, mas dependendo do contexto e de como se relacionam com outros dados pessoais, esses dados podem facilmente se tornar dados confidenciais.

Por exemplo, dados de transações de crédito pessoal que indiquem a compra de medicamentos ou o pagamento de uma consulta podem ser considerados sensíveis porque se referem à saúde do indivíduo. O contexto em que os controladores de dados financeiros analisam quais dados serão considerados dados sensíveis é muito importante, pois regras mais rígidas serão aplicadas ao processamento desses dados sob a LGPD.

Antes da LGPD, os dados financeiros já eram protegidos. A Lei do Sigilo Bancário de 2011 (BRASIL, 2001) e regulamentações do BCB, como a Resolução Conjunta do BCB nº, relativa a sigilo, confidencialidade e proteção de dados. Considerando que não há definição específica do termo "dados financeiros pessoais" na legislação, o conceito será construído com base na Lei do Sigilo Bancário, que prevê em seu § 1º que o sigilo das operações ativas e passivas deve ser protegido • Instituições financeiras e seus serviços.

Portanto, levando em consideração os motivos apresentados, para fins deste relatório, tratamos dados financeiros pessoais como qualquer informação sobre uma pessoa física identificada ou identificável (conforme orientação da LGPD) em relação a transações financeiras ativas e passivas, e serviços prestados.

Nesse sentido, tanto o BCB quanto a ANPD terão papel fundamental na fiscalização da gestão da anuência das instituições que fazem parte do Open Banking e na transparência com os titulares, garantindo que as instituições obtenham a anuência dos titulares e demais disposições complementares de acordo com a LGPD.

Dessa forma, é necessário que as leis e regulamentos conversem entre si, para evitar erros normativos, principalmente para que agências maliciosas encontrem brechas em leis ou regulamentos para processar dados pessoais que sejam inconsistentes com os motivos apresentados pela LGPD. qualidade dos dados, transparência e não conformidade Aplicabilidade do princípio da discriminação.

Em seu artigo 6º, a LGPD vincula seus principais objetivos e linhas de atuação a princípios comuns existentes em diversos ordenamentos jurídicos (Brasil, 2010). Neste artigo, a lei estabelece 10 fundamentos para nortear suas disposições da LGPD, afirmando que o tratamento de dados pessoais deve ser pautado pela boa-fé e pelos seguintes princípios: finalidade, suficiência, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, Não Discriminação e Responsabilidade e Prestação de Contas (Brasil, 2020).

Por exemplo, a LGPD contém disposições que sustentam a necessidade de tratamento de dados para uma finalidade lícita, específica, clara e informada (princípio da necessidade), e que tal tratamento deve ser realizado de forma compatível (princípio da adequação) para informar os titulares da finalidade (princípio da transparência).

Além disso, em cada operação de tratamento, os dados devem ser mantidos precisos, claros, relevantes e atualizados

(Princípio da Qualidade dos Dados), respeitando o facto de que o tratamento dos dados não se destina a fins discriminatórios ilícitos ou abusivos (Princípio da Não -Discriminação, Conformidade Discriminação). Especificamente, levando em consideração os temas abordados neste relatório, bem como a Resolução Conjunta BCB 4.658/2018, seguiremos os princípios de qualidade de dados, transparência e não discriminação também mencionados no artigo 4º da Resolução, artigos I, III e inciso IV.

O princípio da transparência está intimamente relacionado ao relacionamento de uma instituição financeira com seus clientes, pois garante aos titulares não apenas informações claras e precisas, mas também específicas e verdadeiras. Além disso, ainda que os segredos comerciais e industriais sejam protegidos, eles não devem se sobrepor aos direitos dos titulares e demais princípios e princípios fundamentais da LGPD.

A transparência do titular será um dos principais pontos de observação para o bom funcionamento do Open Banking, e será um desafio em primeiro lugar, pois está diretamente relacionado com a gestão eficaz do consentimento do titular e a necessidade de otimizar as atividades de dados de mapeamento para garantir que os titulares clear saiba exatamente como seus dados pessoais são processados.

A qualidade dos dados também é outro aspecto que deve ser observado com muita cautela no contexto do open banking, principalmente nos temas relacionados à relevância e minimização de dados. Isso exigirá que os controladores de dados criem procedimentos rigorosos de verificação contínua para a precisão, clareza, relevância e atualização dos titulares dos dados.

O objetivo é ser fiel à finalidade terapêutica que informa o titular dos dados e evitar algoritmos que utilizem dados imprecisos, desatualizados e irrelevantes para tomar decisões automatizadas. O foco na qualidade dos dados está fielmente vinculado ao princípio da não discriminação, pois a baixa qualidade dos dados afeta não apenas a igualdade entre os indivíduos, mas outros direitos fundamentais protegidos não apenas pela LGPD, mas também pela Constituição Federal. No entanto, o efeito mais visível e mais estudado relacionado aos direitos afetados pela má qualidade dos dados é a não discriminação. Vários estudos e relatórios envolvem o uso de dados não representativos ou algoritmos tendenciosos que tratam as pessoas de forma desigual com base na cor da pele, raça, gênero, orientação sexual, religião e muito mais.

Portanto, se medidas estruturadas que valorizam a qualidade dos dados não forem criadas e a necessidade e adequação do tratamento não forem validadas, o resultado da tomada de decisão automatizada pode diferenciar as pessoas com base em seus dados confidenciais. Numa perspectiva de open banking, os dados relativos à cor da pele, género e origem podem influenciar ainda mais as decisões sobre a concessão de crédito por parte das instituições financeiras (França, 2019).

Foram publicadas notícias sobre a descoberta do machismo e da replicação racista por algoritmos, principalmente no mercado bancário. 55 Como todos os dados das instituições financeiras são consolidados, o direito à não discriminação pode ser mais afetado, maximizando o viés sistêmico.

Com isso em mente, os reguladores não devem se concentrar apenas nos dados pessoais em si, mas também devem desenvolver métodos para educar tanto o público quanto o privado sobre como os algoritmos relacionados aos sistemas abertos bancários abertos funcionarão, para que a base dos algoritmos - dados - possa ser limitado pela legislação e pela lógica, princípios e limitações dos regulamentos. Mais uma vez, a supervisão por parte das autoridades públicas será crucial.

CONCLUSÃO

Como o Open Banking pressupõe o consentimento, que é um dos fundamentos legais da LGPD, os clientes podem conceder permissão para compartilhar a qualquer momento ou revogá-la. Vale ressaltar que essa aceitação é específica, ou seja, os clientes apenas permitem que determinados dados sejam compartilhados com bancos terceiros, não sendo universalmente aplicável a todos os dados ou a todas as instituições.

Para compartilhar essas informações com outras agências, será necessário coletar um novo formulário de consentimento do titular. Isso significa que o órgão receptor dos dados assumirá o papel de controlador perante a LGPD.

Dessa forma, órgãos específicos devem controlar de forma transparente o processo de armazenamento desses dados, além de prestar serviços efetivos e práticos aos titulares dos dados que retirarem seu consentimento ou solicitarem algum esclarecimento sobre o processamento de suas informações. Esse novo processo pode ser facilitado usando um sistema de gerenciamento de relacionamento com o cliente (CRM) e outras ferramentas de gerenciamento.

Criar registros para mostrar como e onde esses dados pessoais são coletados é uma obrigação legal que reflete a importância da transparência para as instituições financeiras. As empresas também devem ter uma política de retenção de informações que atenda aos requisitos legais. Nesse caso, o consentimento será a base legal para reter determinados dados até sua revogação ou expiração.

Portanto, o processamento de dados pessoais se tornará um padrão fundamental que as instituições financeiras precisam considerar ao ingressar no Open Banking. À medida que o mercado bancário inova e deve acompanhar o desenvolvimento de soluções que respeitem a privacidade e protejam os dados pessoais, novos processos e demandas surgirão.

REFERÊNCIAS

BARBERIS, J. N.; BUCKLEY, R. P.; ARNER, D. W. FinTech, RegTech, and the Reconceptualization of Financial Regulation. Northwestern **Journal of International Law & Business,** v. 37, n. 3, 2017.

BARBERIS, J. N.; BUCKLEY, R. P.; ARNER, D. W. The Evolution of Fintech: A New Post-Crisis Paradigm? University of Hong Kong **Faculty of Law Research Paper** No. 2015/047, 20 out. 2015.

BRASIL, Banco Central do Brasil, **Resolução nº 4.658** de 26 de abril de 2018.

BRASIL, Banco Central do Brasil, **Resolução nº4.658** de 26 de abril de 2018. Dispõe sobre a implementação do Sistema Financeiro Aberto (Open Banking).

BRASIL, Banco Central do Brasil. **Resolução Conjunta nº 1** de 4 de maio de 2020.

BRASIL, Lei Complementar nº105, de 10 de janeiro de 2001. **Lei do Sigilo Bancário.** Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências

BRASIL. **Escola Nacional de Defesa do Consumidor** A proteção de dados pessoais nas relações de consumo: para além da informação creditícia / Escola Nacional de Defesa do Consumidor; elaboração Danilo Doneda. – Brasília: SDE/DPDC, p. 43, 2010.

BRASIL. Governo Federal. **Guia de Boas Práticas para Implementação na Administração Pública Federal.** 1 v.11, 2020.

BRASIL. Governo Federal. **Guia de Boas Práticas para Implementação na Administração Pública Federal.**1 v.21,2020

CUEVA, Ricardo Vilas Boas. A insuficiente proteção de dados pessoais no Brasil. Revista de Direito Civil Contemporâneo-RDCC: **Journal of Contemporary Private Law**, n. 13, p. 61, 2017.

DENZIN, N.; LINCOLN, Y. **Handbook of Qualitative Research.** London: Sage Publication Inc, 2000.

EUROPA. EDPS. **Guidelines on data protection in EU financial services regulation**. p. 5

FRANCE. European Union Agency for Fundamental Rights. Data quality and artificial intelligence–mitigating bias and error to protect fundamental rights. p. 8, 2019

GOETTENAUER, C. Open Banking e o Modelo de Banco em Plataforma: a necessidade de reavaliação da definição jurídica de atividade bancária. Revista da Procuradoria-Geral do Banco Central, [S.l.], v. 14, n. 1, p. 13-27, set. 2020

KÖCHE, J. C. **Fundamentos de Metodologia Científica:** teoria da ciência e iniciação à pesquisa. 29. ed. Petrópolis: Vozes, 2011.

MAGNUSON, W. J. Regulating Fintech. **Vaderbilt Law Review,** 2017

MARCONI, M. A.; LAKATOS, E. M. Fundamentos de metodologia científica. 7.ed. São Paulo: Atlas, 2010.

MARTINS, Leonardo (Org.). Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. Montevidéu: **Fundação Kontad Adenauer**, 2005, pp. 233-235

REYNOLDS, Faith. **Open Banking:** a consumer perspective. UK Open Banking, p. 18-19, 2017.

SHANK, G. Qualitative Research. **A Personal Skills Aproach**. New Jersey: Merril Prentice Hall. 2002.

VIOLA, M.; HERINGER, L. A Portabilidade na Lei Geral de Proteção de Dados. **Instituto de Tecnologia e Sociedade,** 2020.