

ESCOLA DE DIREITO  
CURSO DE DIREITO

RICARDO RÖWER DE OLIVEIRA

***OPEN BANKING:***  
**SEUS IMPACTOS NAS RELAÇÕES DE CONSUMO E OS DESAFIOS À PROTEÇÃO DE**  
**DADOS PESSOAIS**

Porto Alegre  
2021

GRADUAÇÃO



Pontifícia Universidade Católica  
do Rio Grande do Sul

# **OPEN BANKING: SEUS IMPACTOS NAS RELAÇÕES DE CONSUMO E OS DESAFIOS À PROTEÇÃO DE DADOS PESSOAIS**

Ricardo Röwer de Oliveira\*

Flávia do Canto Pereira\*\*

## **RESUMO**

Este artigo tem como objetivo elucidar o advento do *Open Banking* no Brasil e o seu contexto de desenvolvimento. Mostrar o seu conceito e sua relevância no sistema financeiro atual e seus efeitos nas relações de consumo assim como a proteção de dados a partir da Lei Geral de Proteção de Dados ou LGPD. O *Open Banking* entre uma série de propostas, esteve entre as essenciais alternativas para ampliação de oferta de produtos mais competitivos para o mercado bancário em geral resguardando os direitos dos consumidores. É importante destacar os diversos benefícios que a maior possibilidade de escolhas trará aos consumidores na tomada de decisão e no controle de seus próprios dados. Neste ponto, se destaca o papel no ambiente regulatório inserido e proposto pelo Banco Central do Brasil e os requisitos fundamentais para sua implementação como peça chave e central deste processo. Em seguida, se estuda neste ambiente cada vez mais tecnológico, os impactos nas relações de consumo e a importância da boa-fé e a confiança nas relações contratuais. É de extrema relevância a proteção da confiança do consumidor como maneira a preencher a lacuna da desconfiança básica entre as partes fortes como as fracas da relação. Neste contexto, é abordado os principais desafios levantados pela doutrina, sejam tanto no campo consumerista quanto ao que tange a proteção de dados e sua observância a lei geral de proteção de dados. Conclui-se que o *Open Banking* deve ser analisado tanto nas questões apontadas na doutrina jurídica, os cuidados no trato com o consumidor do ponto de vista jurídico e os preceitos elencados na segurança da formação e proteção de dados para que possa ocorrer sua efetiva aceitação e sucesso de implementação tanto pelas instituições financeiras quanto pelo consumidor.

**Palavras-chave:** *Open Banking*; LGPD; proteção de dados; consumidor.

## **1 INTRODUÇÃO**

O referido artigo abordará a implementação do *Open Banking* no Brasil e sua dinâmica envolvida no sistema financeiro assim como sua relação no campo das relações de consumo e a proteção de dados a partir da LGPD. O conceito da matéria é amplo e vincula-se diretamente à mudança na estrutura tecnológica das instituições bancárias e no seu modelo de negócio. Buscaremos, assim, destacar as premissas que envolvem seu uso no ecossistema tecnológico e financeiro.

Por consequência, identificamos também diferentes desafios para além da implantação do *Open Banking*, e seu sucesso como ferramenta de desenvolvimento em prol de um campo mais fértil e uma maior competitividade ao consumidor, tendo especialmente cuidados no âmbito da proteção dos dados pessoais.

É sabido que o *Open Banking* propiciará, portanto, diversos benefícios ao consumidor, desde a oferta de serviços mais customizados, adequados, competitivos e, sobretudo, de maior possibilidade de escolha ao cliente na tomada de decisão e no controle de

---

\* Graduando do curso de Direito da Pontifícia Universidade Católica do Rio Grande do Sul. E-mail: ricardo.rower@yahoo.com

\*\* Pós doutoranda em Direito na Universidade Federal do Rio Grande do Sul, Doutora e Mestre em Direito pela PUCRS. Visiting Scholar na Syracuse University. Professora da Escola de Direito da PUCRS. E-mail: flavia.pereira@pucrs.br

de seus próprios dados. Buscaremos, nesta linha, analisar o ambiente regulatório proposto pelo Banco Central do Brasil e, a partir de seus comunicados e resoluções referentes ao Sistema Financeiro Aberto (ou *Open Banking*) e os requisitos fundamentais para a sua implementação. Também levantaremos os principais desafios levantados pela doutrina, sejam tanto no campo consumerista quanto na proteção de dados.

Entre as questões suscitadas, uma das principais provocações apontadas diz respeito à dicotomia entre o fluxo de dados e a necessidade de proteção dos mesmos. Busca-se, assim, analisar, com base na legislação e doutrina, desde o processo de abertura dos dados pessoais até sua dinâmica no âmbito dos contratos bancários. Portanto, a ideia deste artigo é identificar as questões apontadas pela doutrina jurídica, os cuidados no trato com o consumidor do ponto de vista jurídico e os preceitos elencados na segurança da informação e proteção de dados.

No primeiro tópico será abordado o conceito de *Open Banking* e como foi constituído seu modelo regulatório onde analisaremos tanto as principais resoluções postas pelo Banco Central do Brasil quanto as do Conselho Monetário Nacional que foram implantadas e como estas poderão, a critério, estender futuramente a obrigação de adoção do *Open Banking*.

Avaliaremos onde a ferramenta já foi implantada no contexto global, mostrando as razões e principais características elencadas nestes lugares que trouxeram as relevantes premissas para o modelo brasileiro. A LGDP, baseada em parte no modelo europeu de proteção de dados, trouxe padrões e guias de condições iniciais, para evitar os maiores riscos do ecossistema de *Open Banking*, como apontados de quebra ou vazamento de dados, pagamentos não autorizados e erros de processamento.

Assim, dentre uma série de propostas, que foram incluídas nestes lugares, o *Open Banking* esteve entre as essenciais alternativas para ampliação de oferta de produtos mais competitivos para no mercado bancário. O Brasil procurou, em linhas gerais, as mesmas bases e com desafios igualmente elucidados de trazer maior competitividade ao sistema resguardando os direitos dos consumidores, ainda que haja considerações que serão abordadas.

No segundo tópico, falaremos dos impactos do *Open Banking* nas relações de consumo, abordaremos o surgimento de novos negócios e produtos bancários advindos dessa transformação tecnológica, onde os clientes cada vez mais são atendidos pela internet.

Também trataremos sobre a importância da boa-fé e a confiança nas relações contratuais, que são princípios e base da relação de consumo. A confiança é princípio inerente de todo o direito nesta evolução valorizando a confiança depositada no vínculo, as expectativas e a boa-fé das partes contratantes. É relevante a proteção da confiança do consumidor como maneira a complementar preencher a lacuna da desconfiança básica entre as partes e viabilizar o resultado tanto entre as partes fortes como as fracas da relação. Ainda caso algo fuja de tal percepção, também devem os mesmos serem resguardados na atuação e proteção dos demais agentes envolvidos para criar confiança.

Ainda no mesmo tópico serão identificados os desafios levantados pela doutrina à proteção dos dados pessoais e a ameaça quanto ao sigilo bancário e os riscos cibernéticos que foram potencializados neste ambiente. Importante citar que, mesmo com as diversas e inúmeras vantagens que podem trazer o *Open Banking* aos clientes e a comunidade financeira em geral, sua prática enseja também potenciais riscos, como os que serão elencados principalmente no âmbito da proteção de dados e sua relação com o sigilo bancário.

A partir da leitura de dispositivos, será possível analisar os itens jurídicos e normativos e os textos doutrinários. Onde serão analisadas as regras cabíveis para a atribuição de responsabilidade no caso de ocorrer a violação à proteção dos dados pessoais nos contratos bancários. Assim, mostraremos que as legislações aplicáveis buscarão na medida do possível, conforme exposto, conciliar o interesse do titular dos dados, ou seja, aquele que é o cliente em geral, com os interesses daqueles que intermediam nos aspectos econômico e financeiro, com

base nos princípios e fundamentos que norteiam a Lei Geral de Proteção de Dados e traçando um paralelo com os dispositivos já existentes na legislação.

## 2 OPEN BANKING NO BRASIL

O primeiro tema abordado neste capítulo é o *Open Banking* e demais assuntos relacionados, tais como seu conceito e surgimento, como se deu o modelo de regulação de acordo com os órgãos brasileiros da área, entre outros itens.

### 2.1 O conceito, surgimento do *Open Banking* no Brasil

A referida expressão foi adotada pela comunidade financeira, onde haja possibilidade e ingresso de terceiros no ambiente virtual da Internet para intercâmbio de dados, em especial, as relacionadas de uso final ao ecossistema do mercado financeiro.

O sistema pode ser entendido como de compartilhamento de dados a partir da permissão do cliente, de produtos e serviços pelas instituições participantes, por meio de abertura e integração de plataformas de pagamentos em tempo real, dando maiores opções de transparência e oportunidades de marketing e venda<sup>1</sup>.

O conceito da matéria é amplo e usado em diversas ocasiões. Define-se que o surgimento do nome vincula-se diretamente à mudança na estrutura tecnológica das instituições bancárias e no seu modelo de negócio<sup>2</sup>. É possível entender que, até então, os meios onde as transações financeiras ocorriam eram fechados e com dedicação exclusiva do sistema bancário.

Já se vem discutindo e se confirmando, a cada dia, o surgimento de um novo ecossistema<sup>3</sup> de serviços financeiros, cada vez mais intenso e que se torna parte do nosso dia a dia. Esta tendência de ampliação dos meios digitais promove uma revolução no mercado financeiro (WINTER, 2017, p. 32). Nota-se não apenas de novos produtos e serviços que surgem rapidamente, como também o nascimento de novos agentes no sistema financeiro.

Um desses atores que estão transformando completamente o modelo de banco como conhecemos são as *fintechs*<sup>4</sup>, ou seja, *startups* voltadas para modelos inovadores de serviços financeiros utilizando alto grau de recursos tecnológicos. Com o advento deste fluxo intenso de informações, desenvolvimento da tecnologia os canais digitais ampliaram a sua participação em relação aos canais tradicionais: seis em cada dez transações bancárias já são realizadas pelo cliente pelo celular ou pelo computador (FEBRABAN, 2019, p. 10).

Os principais exemplos já inseridos neste contexto são os empréstimos, seguros, investimentos, meios de pagamentos e plataformas de gestão financeira. Vários bancos privados, os chamados “bancões”, também contam com iniciativas para correr atrás, viabilizando através da aceleração e investimentos na área.

<sup>1</sup> Bank of International Settlements (sediado na Basileia/Suíça) conhecido como “banco central” dos bancos centrais.

<sup>2</sup> De modo a também conceituar e entender o termo, o mesmo autor acrescenta: “A incorporação de novas tecnologias trouxe a tona, entretanto demanda pelo uso de aplicações digitais, que se realizam por meio de transações bancárias pela internet, em redes abertas [...]”. Ainda, “O uso da expressão pela imprensa intensificou-se a partir da adoção, pelas autoridades britânicas e europeias, de marcos regulatórios que implicavam padronização da arquitetura tecnológica de instituições financeiras, a fim de garantir o acesso de outros agentes ao mercado”. (GOETTENAUER, 2018, pag.111).

<sup>3</sup> Ecossistema das *fintechs* brasileiras: exemplos: Empréstimos (Creditas); meios de pagamento (Pag Seguro, NuBank); Investimentos: (Investeapp, Smarttbot); Gestão Financeira (Guia Bolso, Conta Azul). (WINTER, 2017, p. 32).

<sup>4</sup> *Fintech*: a palavra *fintech* é uma abreviação para *financial technology* (tecnologia financeira, em português). Ela é usada para se referir a startups ou empresas que desenvolvem produtos financeiros totalmente digitais, nas quais o uso da tecnologia é o principal diferencial em relação as empresas tradicionais do setor. (REDAÇÃO NUBANK, 2020, *online*).

O sistema tem o objetivo de proporcionar a criação de um ambiente mais aberto e competitivo entre as instituições financeiras e as chamadas *fintechs*. Para Müller (2005), durante os anos 90 tínhamos um ambiente bancário bastante distorcido<sup>5</sup>. Assim, devido a fusões e aquisições, tivemos uma grande concentração no sistema financeiro nacional, a despeito do que acontece em vários países, com praticamente 5 instituições financeiras dominando o mercado<sup>6</sup>. Importante destacar que, naquele momento, a ideia central era pela busca de estabilização do sistema financeiro brasileiro, facilitando a concentração e robustez das instituições em ambiente muito fragilizado, pós período de hiperinflação vivido no país. Entretanto, essa concentração trouxe também um difícil acesso à competitividade de produtos e serviços. Por consequência, de comum senso, isso eleva a taxa de juros e preço dos serviços relacionados e oferecidos ao consumidor [...] <sup>7</sup>.

Destaca-se nesta perspectiva que com o advento das tecnologias existentes [...] <sup>8</sup>, a ideia central é que o *Open Banking* seja uma plataforma onde os dados sobre clientes, produtos e serviços fluam no sistema financeiro de maneira padronizada. Além disso, um dos pontos centrais é o perfil do consumidor que, de uma maneira geral, está mudando assim como percebido em outros países. Cada vez temos mais profissionais liberais, trabalhadores individuais, informais, sendo que seus proventos vêm de diferentes formas e fontes (BANK OF ENGLAND, 2020, p. 4, tradução nossa) e as instituições não enxergam esse todo.

De tal modo, essa troca de informação do cliente, tem seu pilar, conforme o pesquisador Bioni, a partir do consentimento [...] <sup>9</sup>, o qual foi ratificado como premissa na sua implantação pelo Banco Central do Brasil (2021). Pode-se, portanto, se o mesmo desejar e consentir, consultar outras instituições, que poderão ofertar possibilidades ou melhores condições em novos produtos ou até cotação dos produtos já contratados (ex: financiamento imobiliário, veículos, etc.).

A possibilidade de ofertar essa análise de maneira padronizada pode mostrar que determinado perfil é mais valorizado em outra instituição. Ou seja, o cliente passa a deter suas informações, desde seu relacionamento, adentrando em questões como seu histórico junto às mesmas, revelando sua capacidade de repagamento no tocante a produtos e serviços contratados, sua performance e características em geral.

Portanto, essa possibilidade quebra ou viabiliza que, não somente os grandes e tradicionais bancos ou aqueles que tenham primordialmente o relacionamento progressivo, permaneçam detentores da informação ou dados sobre o cliente.

---

<sup>5</sup> “Num ambiente de inflação elevada e crescente, permeado por crises internacionais que marcaram a economia brasileira entre a segunda metade dos anos 80 e meados dos anos 90, construiu-se um sistema bancário caracterizado por uma série de distorções [...] A redução do setor como um todo significou a quebra dos menos eficientes e a deflagração de um processo de fusões e aquisições (consolidação). Este processo de reestruturação resultou no desaparecimento, fusão ou incorporação de mais de 50 bancos, ou 20% do total antes existente.”

<sup>6</sup> “The banking sector plays a central role in the functioning of the economy [...] and it is extremely concentrated: averaging across countries, the share of assets held by the 5 largest banks in each country is 78%, a number that has increased recently in several countries.” (JOAQUIM; DOORNIK; ORNELAS, 2019, p. 6, atualizado em maio de 2020).

<sup>7</sup> “O debate acerca do papel da concorrência na indústria bancária remete ao conhecimento comum de que em um ambiente não competitivo podem ocorrer perdas de bem-estar. Bancos com poder de mercado exercerão este poder para obter maiores lucros cobrando juros mais elevados e remunerando os investimentos a menores taxas [...]” (MÜLLER, 2005, p. 88).

<sup>8</sup> “[...] advento do internet banking, que foi sucedido pela criação do mobile banking. Atualmente, fala-se em quarta revolução industrial, como um período de mudança dos mercados de forma geral, nos quais preponderam a tecnologia e o valor econômico de dados.” (BROLLO; ALMEIDA, 2020, p. 196).

<sup>9</sup> “O consentimento é o pilar regulatório adotado para a proteção de dados pessoais. A regra geral é a de que o cidadão deve consentir para que haja fluxo de suas informações pessoais, sendo essa a razão da extensa adjetivação empregada como: livre, expresso, específico e informado”. (INTERNETLAB PESQUISA EM DIREITO E TECNOLOGIA, 2016, p. 93).

O sistema desenvolvido conta com as instituições financeiras autorizadas pelo Banco Central e este também como guardião das informações e regulador do projeto no Brasil (OPEN BANKING BRASIL, 2021). A ferramenta irá possibilitar, portanto, o compartilhamento das informações pelo usuário de maneira clara e totalmente digitalizada tendo como premissa a busca de padrões de segurança e de acordo a lei geral de proteção de dados (LGPD).

Todo este compartilhamento será possível em termos amplos por mecanismos que consistem nos chamados APIs<sup>10</sup>. Nem todos os sistemas conversam entre si, não possuindo a mesma programação, mas o *Open Banking* implementa a ligação e converte as diferentes linguagens, trazendo, assim, a possibilidade de compartilhar os dados necessários e a integração através dos sistemas, plataformas e infraestrutura (BANK OF INTERNATIONAL SETTLEMENTS, 2019, p. 19).

## 2.2 A regulamentação e a experiência internacional

O Bacen, em 2019, tendo como premissas a promoção de um amplo processo de democratização, rebatizou seu programa, passando a chamar-se “Agenda BC#<sup>11</sup>”. Em linhas gerais, a busca da democratização do sistema financeiro conta com quatro itens centrais, que passaram a nortear as suas diretrizes: inclusão, competitividade, transparência e educação. O *Open Banking* está inserido no item “competitividade” (BANCO CENTRAL DO BRASIL, 2020b).

A ação visa acolher no sistema financeiro alta tecnologia possibilitando maior inclusão no mesmo. Cabe mencionar que o atual presidente da autarquia destacou a relevância do tema<sup>12</sup> durante sua sabatina no Senado Federal<sup>13</sup>.

Pondera-se neste sentido, que são amplos os efeitos nesse novo modelo de negócio, onde empresas de médio e pequeno porte entram na relação entre bancos e clientes, o que resulta em novas formas de concorrência [...] <sup>14</sup>.

O Banco Central do Brasil (BACEN) vem, nos últimos anos, promovendo e incentivando a inserção e a competitividade. A autarquia, nesta linha, divulgou no comunicado nº 33.455 em abril de 2019, referente ao Sistema Financeiro Aberto (ou *Open Banking*) os requisitos fundamentais para a sua implementação.

Primeiramente houve um processo, tanto para o acolhimento de sugestões quanto outras questões pertinentes anteriormente mencionadas, trabalho que culminou em maio de 2020. Onde, em conjunto, tanto o conselho monetário nacional quanto a diretoria colegiada do BACEN elaboraram a Resolução Conjunta 01/2020<sup>15</sup>, a qual dispõe sobre a implementação do

---

<sup>10</sup> *Application programming interface*: em termos menos técnicos, nada mais é do que uma parte ou “camada” nos sistemas que funciona como uma interface para troca das informações, e esta permite que os diferentes sistemas possam dialogar entre si.

<sup>11</sup> Para saber mais, Agenda BC# completa em: <https://www.bcb.gov.br/acessoinformacao/bchashtag>. (BANCO CENTRAL DO BRASIL, 2020a?).

<sup>12</sup> Ainda destacou que: “novas tecnologias como blockchain, o uso de inteligência artificial, identidade digital, pagamentos instantâneos, *Open Banking*, dentre outras inovações, estão alterando completamente os modelos de negócios e os serviços financeiros”. (CAMPOS NETO, *apud* MARTINS, 2019, *online*).

<sup>13</sup> “[...] o mundo passa atualmente por uma onda de inovação e mudanças. É crucial pensar hoje em como será o sistema financeiro no futuro e preparar o Banco Central do Brasil para desempenhar apropriadamente suas funções nesse novo ambiente, que será certamente baseado em tecnologia e no fluxo rápido de informação [...]”. (CAMPOS NETO, *apud* MARTELLO, 2019, *online*).

<sup>14</sup> “[...] as consequências desse novo modelo de negócio, com a inclusão de empresas intermediárias na relação entre cliente e instituição financeira, são vastas e têm influência especial sobre a estrutura do mercado financeiro, com repercussões diversas como as de caráter concorrencial [...]”. (GOETTENAUER, 2018, p.113).

<sup>15</sup> Resolução conjunta 01/2020 – Banco Central do Brasil, possui um total de 55 artigos regulamentando o *Open Banking* no Brasil (BANCO CENTRAL DO BRASIL, 2020c).

Sistema Financeiro Aberto e a Circular BACEN 4.015/2020, que versa sobre o escopo de dados e serviços do modelo no Brasil.

Em síntese, o artigo 4º da Resolução Conjunta 01/2020 (BANCO CENTRAL DO BRASIL, 2020c) norteia o Sistema Financeiro Aberto, destacando os principais itens como (a) transparência; (b) segurança e privacidade de dados e informações compartilhados; (c) qualidade dos dados; (d) tratamento não discriminatório; (e) reciprocidade; e (f) interoperabilidade. Ainda, no artigo 5º, a resolução infere sobre dados, produtos e serviços que serão cobertos pelo *Open Banking* (cadastros de clientes, transações financeiras e canais de comunicação). Posteriormente, conforme Brollo e Almeida (2020), destaca-se a questão do compartilhamento das informações no sistema (art. 10), onde cabe inferir que será vedada qualquer autorização por meio do chamado contrato de adesão (art. 10, § 3º), garantindo, ainda conforme (art. 15), que o titular possa a qualquer momento revogar a mesma<sup>16</sup>.

Tanto o Bacen quanto o Conselho Monetário Nacional (CMN) colocaram que somente as instituições dos segmentos principais e mais representativos<sup>17</sup> estarão obrigadas, neste momento, ficando facultadas as demais à adesão (cf. art. 6º da Resolução Conjunta 01/2020). Cabe ainda inferir, entretanto, que a mesma resolução poderá, a critério da própria autarquia, estender futuramente a obrigação. Ainda, outras regulamentações e obrigações estão elencadas tais como possibilitar suporte técnico através de canais (art. 30) e nomeação de responsáveis pelo compartilhamento (art. 32).

Brollo e Almeida (2020, p.197) comentam que, “[...] além dessas premissas, já se notou de início a natural preocupação com a proteção de dados pessoais [...]”. Estas, portanto, já foram criadas e alinhadas em consonância com a Lei 13.709, a Lei Geral de Proteção de Dados. Assim, há expressa responsabilidade por parte das instituições participantes, seja tanto pelas questões de integridade, disponibilidade, confiabilidade, sigilo e segurança e por todos os dados que venham a ser divididos ou compartilhados, tão bem como da legislação pertinente em vigor<sup>18</sup>.

Logo, as partes envolvidas na temática, sob as mais diversas hipóteses, não poderão indiscriminadamente compartilhar tais dados e informações, pois terão que observar o dever de tratamento e seguir as diretrizes da LGPD em toda a sua cadeia, englobando qualquer tratamento com esses dados pessoais, desde seu acesso, coleta, distribuição, guarda, modificação e qualquer das outras possibilidades existentes ou criadas futuramente, em linha com o art. 51 da referida lei<sup>19</sup>.

Observa-se que é possível delinear a parte regulatória (parte de encargo do BACEN) e a outra chamada de autorregulação, a encargo dos participantes no que tange a padrões de tecnologia destacados nos artigos (art. 44, I), governança (art. 44, VIII, § 1º), segurança e desenho de interface (art. 44, I, “a”, item 1), por exemplo, devem ser organizados entre os

<sup>16</sup> “Art. 15 [...] § 1º Para os fins do disposto no caput, as instituições devem disponibilizar ao cliente a opção da revogação de consentimento ao menos pelo mesmo canal de atendimento no qual foi concedido, caso ainda existente. [...] § 3º A revogação de que trata o caput deve ser efetuada com observância dos seguintes prazos: I - em até um dia, contado a partir da solicitação do cliente, no caso do compartilhamento de serviço de iniciação de transação de pagamento de que trata o art. 5º, inciso II, alínea ‘a’; [...]; II - de forma imediata, para os demais casos”.

<sup>17</sup> Basicamente esses segmentos são as instituições financeiras mais representativas no sistema financeiro nacional em termos de volume, segmento S1: onde os bancos representam ser iguais ou maiores que 10% do PIB brasileiro (ou atividade internacional relevante) e o segmento S2, que compreendem aqueles com tamanho entre 1% a 10% do PIB nacional. (BANCO CENTRAL DO BRASIL, 2021b, *online*).

<sup>18</sup> Os autores supracitados ainda colocam que “[...] Ao lado dos benefícios que são esperados da implementação do *Open Banking* no país, existe a preocupação com a proteção de dados compartilhados, assim como com o tratamento que a eles será conferido pelas instituições participantes do sistema”. (BROLLO; ALMEIDA, 2020, p.195).

<sup>19</sup> Lei 13.709, a Lei Geral de Proteção de Dados Pessoais (LGPD) traz: “Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.” (BRASIL, 2018).

agentes. Se prevê ainda, conforme art. 46, que o próprio BACEN conduz inicialmente a governança do processo, podendo, assim, ser chamada de autorregulação assistida<sup>20</sup> neste momento (DAMASO, *apud* TAIAR, 2020, *online*).

Em especial no Reino Unido, o *Open Banking* teve seu estímulo de implantação, quando a autoridade britânica responsável pelo controle da concorrência “CMA”<sup>21</sup> constatou que os bancos de maior porte e mais tradicionais não necessitavam competir pelos clientes. Em contrapartida, os entrantes ou menos consolidados tinham muitas dificuldades. Assim, dentre uma série de propostas, incluía o *Open Banking*<sup>22</sup>.

Ainda, com sua implementação, em 2018, os bancos europeus receberam a regulamentação para abertura de suas plataformas com base na *General Data Protection Regulation*<sup>23</sup> (Regulamento Geral sobre Proteção de Dados), que foi aprovado pela União Europeia. O Brasil procurou, em linhas gerais, as mesmas bases e com desafios igualmente elucidados de trazer maior competitividade ao sistema resguardando os direitos dos consumidores, ainda que haja considerações para Mendes e Bioni (2019)<sup>24</sup>.

Cabe ressaltar que a norma em vigor na União Europeia é a Diretiva (EU) 2015/2366 do Parlamento Europeu, de 25 de novembro de 2015 (chamado de *Second Payment Services Directive – PSD2*)<sup>25</sup>, resolução esta que entendeu que o mercado de serviços de pagamento e transações financeiras estava mais robusto e complexo, gerando por consequência lacunas à segurança jurídica de tudo que fosse inovador em termos de serviços financeiros. Podendo, assim, lhe ser ofertado mais opções por maior número de empresas. Ainda, a PSD2 trouxe padrões e guias de condições iniciais, para evitar os maiores riscos do ecossistema de *Open Banking*, como apontados de quebra ou vazamento de dados, pagamentos não autorizados e erros de processamento<sup>26</sup>.

Já, em termos de implantação, o modelo brasileiro se assemelha mais ao que foi adotado pela autoridade Monetária de Hong Kong, entre as quais adotou o sistema e edição de regulamentação de APIs (*application programming interface*), com especificações técnicas abertas facilitando a adoção das práticas do *Open Banking* (BANK OF INTERNATIONAL SETTLEMENTS, 2019, p. 11) a qual previu a implementação faseada, assim como está acontecendo no caso brasileiro (fase I, II, III, IV)<sup>27</sup>.

<sup>20</sup> “[...] quanto a visão geral de autorregulação, cumpre mencionar que ela deverá ser proposta pelos participantes do sistema e aprovada pelo CBC, estabelecendo normas e regras de conduta, de forma a complementar e aprofundar a regulação do BCB e do Conselho Monetário Nacional” (RIBEIRO; BAGNOLI, 2020).

<sup>21</sup> Competition and Markets Authority – órgão governamental no Reino Unido responsável em identificar problemas de competitividade no país (leis de proteção de consumo, competitividade mercados, regulação e possui funções do CADE – Conselho Administrativo de Defesa Econômica no Brasil). (UNITED KINGDOM, 2021?).

<sup>22</sup> Neste sentido, coloca que o *Open Banking* no Reino Unido, com quase 4 anos, o progresso está mais lento que o esperado uma vez que enquanto os grandes bancos, inicialmente assustados em perder mercado, conseguiram atender a premissas de segurança de melhor forma que as *fintechs* em geral. (ROBINSON, 2021).

<sup>23</sup> Conhecido também pela sigla GDPR.

<sup>24</sup> [...] o autor ainda que considere o modelo brasileiro influenciado pelo modelo europeu, há diferenças substanciais na técnica legislativa entre os regimes da LGPD e da GDPR. A proteção de dados foi incluída como direito fundamental na União Europeia, portanto possui um corpo normativo mais extenso em comparação a LGPD, ainda que convirjam para práticas justas e direitos dos titulares como pilares. (MENDES; BIONI, 2019).

<sup>25</sup> PSD2: regula o serviço de pagamentos no mercado interno europeu, são mais de 117 artigos de regulação inclusive com resolução de disputas e as possibilidades de multas aplicáveis para cada estado da comunidade (THE EUROPEAN PARLIAMENT; THE COUNCIL OF THE EUROPEAN UNION, 2015).

<sup>26</sup> Trecho original: “Payment Services Directive (PSD2) and subsequent guidelines and standards set the authorization requirements for account information and payment initiation services, rules on the access to accounts and the provision of services”. (CARR; URBIOLA; DELLE-CASE, 2018, p. 3).

<sup>27</sup> Fases do *Open Banking* no Brasil: 1ª fase: início em 1/2/2021 – disponibilização informações padronizadas e canais atendimento; 2ª fase: início em 13/08/2021 – compartilhamento de dados cadastrais como contas, crédito e pagamentos; 3ª fase: início em 30/08/2021 – iniciação de transações de recepção de propostas de operações de



### 3 OS IMPACTOS DO *OPEN BANKING* NAS RELAÇÕES DE CONSUMO

O objeto a ser tratado neste item refere-se aos impactos do *Open Banking* nas relações de consumo passando pelo aparecimento de negócios e produtos bancários ocorridos da mudança tecnológica que se sucede, entre outros assuntos.

#### 3.1 A confiança e a boa-fé

O *Open Banking* é consequência de diversas transformações no campo tecnológico, financeiro, do surgimento de *fintechs* e assim como das relações de consumo que inevitavelmente afetam as relações contratuais e seus pilares como o da confiança e a boa-fé. O advento massificado das informações, produtos e serviços, o uso de dados e disponibilidade deles pelos meios eletrônicos evidentemente podem gerar uma percepção de desconfiança aos consumidores.

Além disso, surgiram novos negócios e produtos bancários advindos dessa transformação, onde os clientes cada vez mais são atendidos pela internet. Igualmente, de uma maneira ampla, os contratos de adesão regem as relações bancárias e são guiados pelo CDC.

Assim, a boa fé e a confiança são princípios e base da relação de consumo, onde a confiança é princípio inerente de todo o direito. É também um princípio da diretriz das relações contratuais. A lei protege determinados interesses sociais, valorizando a confiança depositada no vínculo, as expectativas e a boa-fé das partes contratantes<sup>28</sup>.

A proteção da confiança do consumidor é o novo princípio complementar da boa-fé objetiva uma vez que o contrato de consumo, pode preencher a lacuna da desconfiança básica entre as partes e viabilizar o resultado tanto entre as partes fortes como as fracas da relação. A necessidade da confiança e sua proteção nas relações de consumo se tornam neste processo de transformação fator ainda mais imperativo. O contrato ganhou novas formas, os sujeitos contratuais também, assim como as conexões, os protocolos, valorizando-se a sua força e o impacto na criação e quebra de expectativas agora legítimas (MARQUES, 2006).

Ainda que haja previsão, não podemos esquecer os ensinamentos de Marques (2006) onde as decisões no campo do consumo pelos clientes deveriam dar a noção do resultado que se auferem. Entretanto, caso algo fuja de tal percepção, também devem os mesmos serem resguardados na atuação e proteção dos demais agentes envolvidos para criar confiança, destacando-se o princípio da responsabilidade. São bases importantes, portanto, a vontade de um parceiro e a confiança criada no outro nesta relação consumerista.

Nesta linha, as relações bancárias tiveram a inclusão das *fintechs*, que são uma das bases de apoio ao desenvolvimento do *Open Banking*<sup>29</sup>. Destaca-se, ainda, a previsão da Resolução 4.656/2018 do Conselho Monetário Nacional, onde modalidades de *fintechs* de crédito

---

crédito; 4ª fase: início em 15/12/2021 – compartilhamento de informações sobre produtos, previdência, seguros, câmbio entre outros distribuídos no mercado (OPEN BANKING BRASIL, 2021).

<sup>28</sup> Marques (2006) ainda cita, “[...] o Código de Defesa do Consumidor brasileiro realmente impõe a transparência (art. 4.º, caput), o princípio da boa-fé objetiva (art. 4.º, III, CDC) e a ativa proteção do consumidor com base na boa-fé de condutas (art. 51, IV e § 1.º, CDC) e na interpretação dos contratos conforme a confiança despertada (art. 30, 34, 35, 47 e 48 todos do CDC). Em linha, o Código Civil de 2002 (Lei 10.406/2002 (LGL2002/400) cria deveres com base na boa-fé (art. 422, CC/2002), impõe limites (art. 187, CC/2002) e uma interpretação guiada por esta boa-fé objetiva (art. 113, CC/2002) e, em especial, impõe como razão e limite à autonomia privada a função social dos contratos (art. 421, CDC)”.

<sup>29</sup> Neste contexto, a vulnerabilidade do consumidor se demonstra agravada na contratação através do ambiente virtual, uma vez que a simplificação na manifestação do consentimento influencia o contratante a concordar de forma menos refletida com cláusulas que podem ser consideradas abusivas. (VERBICARO; MARTINS, 2018 *apud* PASQUAL; PACHECO, 2019; MARTINS, 2019, p. 200).

admitidas no Brasil passaram ao status de instituições financeiras (BANCO CENTRAL DO BRASIL, 2018b). Trazendo, desde então, repercussões na tutela do consumidor e ratificando que toda pessoa física ou jurídica é considerada consumidora conforme previsto no CDC e assentado na ADIN julgada n. 2.591-DF, chamada de ADIn dos Bancos<sup>30</sup>.

Entende-se, assim, que os consumidores esperem a proteção da lei e, logo, não venham a aceitar falhas, sejam de qualidade, segurança, informação, zelo e cumprimento do acordado. Por consequência, uma vez não preenchidos os pressupostos elencados, venham a exigir futura reparação, mesmo que por danos morais.

Conforme elencado acima, afasta-se qualquer dúvida acerca da aplicação do CDC a estes fornecedores conforme previsto pelo artigo 3º, § 2º e são entendidas como fornecedoras de serviços de empréstimo e crédito em geral. Devem por consequência, garantir a segurança e informação para os clientes [...] <sup>31</sup>, com o dever de boa-fé, características da relação de consumo.

Assim, as questões inerentes ao *Open Banking* devem, hoje, ser lidas e interpretadas em harmonia com os princípios consagrados no CDC como boa-fé e transparência.

Adicionalmente, está presente no nosso sistema jurídico a figura da responsabilidade pré-contratual, ou seja, os agentes envolvidos e responsáveis em ofertar novas soluções financeiras, via *Open Banking*, assim como todos os cuidados na cura dos dados e seu devido uso devem atuar de modo a criar a ideia de que a garantia e cuidado dos mesmos já existem de antemão.

Portanto, para o cliente, este processo já estaria chancelado no consentimento prévio da transmissão de dados ou do aceite de qualquer proposta, onde a vigência desta garantia se dá desde aquele momento. Outra importante consequência prática da aplicação do Código de Defesa do Consumidor às operações realizadas pelas *fintechs* diz respeito ao art. 49 do CDC<sup>32</sup>, em relação ao arrependimento<sup>33</sup>.

Marques (2006) explica que, em relação a confiança, para o consumidor leigo tudo ocorrerá bem, ou seja, seria uma maneira de reduzir a complexidade envolvida na vida contratual. Como também, por outro lado, pode ser usado em sentido contrário. O indivíduo define se aquela oferta ou contexto de consumo merece sua confiança. Como resultado, se depositamos confiança no parceiro contratual, atuamos de forma mais simples e direta, se

---

<sup>30</sup> A ADIN proposta pela Confederação Nacional do Sistema Financeiro em dez/2001, objetivava aclarar a inconstitucionalidade da expressão “inclusive de natureza bancária, financeira, de crédito e securitária” do § 2º do artigo 3º do Código de Defesa do Consumidor, que traz o conceito de serviço, defendendo, desta forma, a não incidência do CDC a tais serviços e inconstitucionalidade formal da aplicação do CDC em razão da violação ao artigo 192, II e IV da CF/88 que previa a regulamentação do SFN através de lei complementar, entendendo não ser possível a aplicação do CDC às instituições financeiras, por se tratar de lei ordinária. A ADIn 2.591 estava sustentada no argumento de que as matérias pertinentes ao SFN deveriam ser objeto de uma única lei, a Lei 4.595/64, que fora recepcionada pela nova ordem constitucional como lei complementar. A ADIN 2.591 foi julgada improcedente, caracterizando um marco no reconhecimento constitucional da proteção do consumidor nas relações bancárias (PASQUAL; PACHECO, 2019).

<sup>31</sup> [...] desta forma, o reconhecimento da aplicação do Código de Defesa do Consumidor às relações estabelecidas entre as instituições financeiras, *fintechs* de crédito e os usuários das plataformas digitais impõe o dever de informação aos fornecedores, que devem garantir que o consumidor exercite o seu poder de escolha de forma informada e consciente (PASQUAL; PACHECO, 2019).

<sup>32</sup> “Art. 49. O consumidor pode desistir do contrato, no prazo de 7 dias a contar de sua assinatura ou do ato de recebimento do produto ou serviço, sempre que a contratação de fornecimento de produtos e serviços ocorrer fora do estabelecimento comercial, especialmente por telefone ou a domicílio. Parágrafo único. Se o consumidor exercitar o direito de arrependimento previsto neste artigo, os valores eventualmente pagos, a qualquer título, durante o prazo de reflexão, serão devolvidos, de imediato, monetariamente atualizados”. (BRASIL, 1990).

<sup>33</sup> O direito a arrepender-se quanto a aquisição de produto ou serviço é previsto pelo CDC aos consumidores que realizam a contratação fora do estabelecimento comercial, uma vez que nestas condições o consumidor estaria mais vulnerável nas relações estabelecidas com o fornecedor (LIMA; SILVEIRA, 2018 *apud* PASQUAL; PACHECO, 2019, p. 201).

confiamos, o contrato em última análise, nem precisaria ser escrito.

O consumidor possui o direito de informação nos termos do artigo 6º, III, do CDC (MARQUES, 2001; PASQUAL; PACHECO, 2019, p. 200). Logo, a modificação das relações de consumo para o âmbito financeiro, como as reforçadas pelo advento do *Open Banking*, só ratificam ainda mais para as instituições financeiras o dever de informar<sup>34</sup> o consumidor, seja sobre os produtos e serviços, o preço e também os termos do contrato assim como das obrigações que está assumindo (arts. 30, 35, 46, 52 e 54, CDC). Ainda, os reguladores devem neste sentido, apoiar e fiscalizar que as partes promotoras destaquem de maneira completa tanto as características, riscos envolvidos como custos de maneira precisa e clara.

O dever de informação torna-se ainda mais imperioso para a proteção na escolha onde o consumidor possui o direito de livre escolha e de liberdade na aquisição de serviços financeiros (MARQUES, 2001). Não se deve admitir, então, omissões ou erro em relação à expectativa levantada nos clientes<sup>35</sup>. Neste sentido, destaca-se o Decreto Federal nº 7.962/2013, onde este define o conteúdo e extensão do dever do fornecedor de informar também no comércio eletrônico [...]<sup>36</sup>.

Inclusive, já tendo o cliente, o direito de receber os benefícios e proteções, e as *fintechs* ou instituições financeiras por sua vez envolvidas não poderão deixar de indenizar prejuízos superveniente sob a alegação de que ainda não fora concretizado o negócio<sup>37</sup>. Razoável, nestas situações, deduzir daí que o cliente ficou com a justa expectativa de estar coberto dos riscos a partir daquele momento.

Neste sentido, percebendo o verdadeiro potencial do *Open Banking*, tanto consumidores e instituições financeiras serão as chaves para ganhar confiança nesta questão, assim como o papel fundamental dos reguladores em apoiarem a inovação e assegurarem os consumidores<sup>38</sup>.

No tocante à questão de supervisão das relações envolvidas neste mercado destaca que a imposição de sanções e possíveis exclusões dos participantes do sistema deverão ser concretizadas pelo BACEN, de acordo com o estabelecido na regulação<sup>39</sup>.

Ainda que, com este alicerce citado, Marques (2006) destaca que vivemos uma nova concepção de contrato de consumo “*a chamada nova crise do contrato e da confiança*”.

Ou seja, vem ocorrendo uma reestruturação da técnica contratual, a exemplo dos contratos de crédito, seguros, licenças, investimentos em bolsa e seus desafios propostos pelo

<sup>34</sup> “Art. 6º São direitos básicos do consumidor: [...] III - a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem” (BRASIL, 1990).

<sup>35</sup> “[...] a comunicação e a informação são os sinais mais importantes de nossos tempos pós-modernos, o paradigma atual do Direito” (MARQUES, 2006).

<sup>36</sup> “[...] O fato de a contratação de consumo se dar por intermédio da internet, caracterizando o denominado comércio eletrônico, não afasta a incidência das normas do CDC, tampouco prejudicam sua aplicação. Deve ainda dispor de meios eficazes para o consumidor identificar e corrigir erros ocorridos nas etapas anteriores à conclusão do contrato, confirmar imediatamente o recebimento da aceitação da oferta, disponibilizar o contrato de modo a permitir sua conservação e reprodução pelo consumidor, além de utilizar mecanismos de segurança eficazes para pagamento e tratamento de dados (art. 4º CDC)” (MIRAGEM, 2019b).

<sup>37</sup> Eventual falha do sistema que sirva de meio aos contratos são compreendidos como de risco inerente à atividade do fornecedor, e deverá o mesmo responder pelos prejuízos que forem causados aos consumidores (MIRAGEM, 2019b).

<sup>38</sup> “A matter of trust. Realizing the true potential of *Open Banking* – both for consumers and financial institutions – hinges on gaining consumer trust. Regulators can play their part by building environments that support innovation and reassure consumers [...]”. (THOMAS, BELLENS e CLAUS, 2020, *Online*).

<sup>39</sup> No que se refere ao suporte aos clientes, a entidade de implementação deverá indicar os procedimentos de suporte ao cliente que as autarquias responsáveis (por exemplo, PROCONS e BACEN) podem seguir para obter subsídios dos participantes do sistema de *Open Banking*. A parte da autorregulação (comentada no item I.II), poderá prever a aplicação de penalidades aos participantes do sistema caso de descumprimento dos padrões e falhas de procedimento, bem como determinar a suspensão temporária em caso de risco/ameaça à segurança do sistema (RIBEIRO; BAGNOLI, 2020).

consumo no comércio eletrônico, onde o intangível e a distância emergem neste contexto. A mesma afirma que os preceitos e concepção de contrato até então tradicionais estão em transformação e em declínio, portanto.

Ainda que isto esteja ocorrendo, elenca-se que o novo paradigma tecnológico do mercado de consumo digital pelas plataformas digitais conta ainda com três pilares básicos semelhantes às relações anteriores i) aquele que é o organizador da plataforma (portanto, aquele que irá intermediar a relação); ii) o que será o fornecedor do serviço e o iii) consumidor<sup>40</sup>.

Nesta transformação referida, Miragem (2019b, p. 19) assim comenta, o sobre os *smart contracts*<sup>41</sup>, onde por inerência a tecnologia aplicada diminuem a interação entre as partes, e o principal aspecto ao comércio eletrônico passa a ser o dever de informar do fornecedor<sup>42</sup>[...]. Com relação ao cliente, para Marques (2006) devem fazer nascer expectativas legítimas naqueles em que despertamos a confiança, ou seja, aqueles que irão receber as informações.

Entretanto, neste novo contexto tecnológico, há a existência de uma cadeia “escondida” de fornecedores, onde os mesmos deverão responder solidariamente quando participam da organização. Esta ideia tem por base a questão da confiança em relação à imagem e informação prestadas. A decisão de consumo do cliente não obrigatoriamente recai sobre o fornecedor e sim sobre a confiança depositada no intermediário em oferecer os respectivos produtos.

Será a confiança na segurança prestada ou eficiência do intermediário (ex: plataforma digital) a verdadeira decisão de contratar do consumidor, motivo que puxa para si sua responsabilidade como organizador (FRAZÃO, 2017<sup>43</sup>; MARQUES, 2017, p. 247-268; 2019, p. 444 *apud* MIRAGEM, 2019b, p. 27).

Por derradeiro, ainda que haja questões complexas e aplicadas na relação de consumo com o advento de novas tecnologias, atualmente, o brasileiro, de maneira geral, está mais aberto ao *Open Banking*, mesmo que possa barrar ainda em questões de infraestrutura<sup>44</sup>.

Ainda, segundo levantamento, os consumidores de maneira geral em países que já desenvolveram o *Open Banking*, estão de fato mais preocupados com a proteção de dados e

---

<sup>40</sup> “[...] a atuação das empresas que organizam essas plataformas digitais também visa, cada vez mais, a coleta e tratamento de dados dos consumidores, visando a seu tratamento, tanto para segmentação de mercado e maior eficiência no direcionamento de ofertas de produtos e serviços, quanto seu compartilhamento com outros fornecedores, na internet e fora dela [...]”. (MIRAGEM, 2019b).

<sup>41</sup> “[...] modo que não apenas sua celebração se dá de modo automatizado (ou mediante aceitação virtual do consumidor), senão também a execução, mediante ordens pré-determinadas que as partes contratantes definem para que se realizem de modo automático, normalmente por intermédio de software que as viabiliza”.

<sup>42</sup> “[...] deve contemplar três aspectos: a) atendimento ao dever de informação e esclarecimento do fornecedor, prévio à contratação, e a possibilidade de acesso prévio ao instrumento contratual (art. 46, do CDC, e art. 4º, IV, do Decreto 7.962/2013); b) assegurar-se a possibilidade de contato do consumidor com o fornecedor por meio alternativo ao da contratação (e-mail, telefone ou endereço físico); c) na programação de suas ordens auto executáveis, assegurar-se que contemplam os condicionamentos definidos pela legislação e resolução no caso de vícios da prestação (arts. 18 a 20 do CDC), assim como o direito de arrependimento (art. 49 do CDC)”.

<sup>43</sup> A autora destaca a interferência direta no serviço ofertado pelos prestadores que ficam sujeitos aos aspectos da qualidade, padronização e preço impostos pelo agente empresarial detentor da plataforma, como pela ótica dos usuários que não têm outra opção senão aceitar a oferta de serviço predeterminado, tal como proposta pelo detentor da plataforma.

<sup>44</sup> Uma alta porcentagem dos consumidores bancários brasileiros tem acesso à internet. No entanto, na maioria dos casos, os serviços são lentos – suficientes para fazer pagamentos digitais, mas inadequados para a maioria dos investimentos online, crédito ou serviços P2P. Apenas 13% da população brasileira tem uma assinatura de internet de banda larga (em comparação com uma média de 39% em todos os países pesquisados [...]) e menos da metade dos consumidores (43%) tem um telefone inteligente (em comparação com 69% dos de outros países). [...] Embora os clientes bancários brasileiros mostrem vontade de adotar uma gama maior de serviços financeiros abertos (*Open Banking*), as melhorias na infraestrutura serão pelo menos tão importantes quanto as mudanças regulatórias na condução da aceitação (SCHUR, 2019).

problemas de *cybersecurity*<sup>45</sup> [...]. Ou seja, esta percepção atual entre fornecedor e consumidor nas relações de boa-fé e confiança recai sobre questões de segurança dos dados.

### 3.2 Observância da Lei Geral de Proteção de Dados e o *Open Banking*

A LGPD objetiva a defesa e proteção dos direitos fundamentais, entre eles o de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural. Tem ainda, entre seus fundamentos, que resguardar o respeito à privacidade, a autodeterminação informativa, a inviolabilidade da intimidade e a defesa do consumidor (BRASIL, 2018). O Objetivo central da LGPD é resgatar a dignidade dos titulares de dados e seus direitos básicos relacionados à autodeterminação informativa (TEPEDINO; FRAZÃO; OLIVA, 2019).

A questão da privacidade é um problema que persegue qualquer questão do desenvolvimento tecnológico, trazendo um novo conceito de privacidade, que corresponderia a pessoa ser detentora exclusiva de suas próprias informações<sup>46</sup>. O advento LGPD traz um avanço para proteção da sociedade, onde os dados são transferidos em meio a tecnologias, redes sócias e diversos meios desta conjuntura (MENDES; DONEDA, 2018).

Para Doneda (2011), a proteção de dados é um direito fundamental, por tratar-se de direito de personalidade. Deve garantir ao indivíduo poder de fato controlar as suas próprias informações, no âmbito das interações entre indivíduo e sociedade. Através desta lei, se reforçam os benefícios, desde a liberdade no controle dos dados pessoais, como o uso incorreto, considerando que a adequação à nova lei, além de mandatária, será fundamental aos negócios em geral (JOELSONS, 2020).

O *Open Banking*, então, parte do princípio de que os dados pessoais e as informações bancárias dos clientes pertencem a estes sujeitos, e não às instituições financeiras, alinhado às premissas da LGPD (PASQUAL; PACHECO, 2019).

Miragem (2019a) destaca, nesse sentido, que a LGPD está relacionada à defesa do consumidor (art. 2º, VI), reforçando a competência dos órgãos de defesa do consumidor por ordem do titular dos dados, se alguma transgressão ocorrer por aquele que é o controlador (art. 18, § 8º), assim como a obrigação de coordenar junto a ANPD<sup>47</sup> e outros órgãos de competência<sup>48</sup>. Ainda, concomitantemente ao CDC, em matéria de não exclusão e acumulação dos direitos e princípios que consagra em relação àqueles estabelecidos em outras leis, destaca-se o art. 64 da LGPD<sup>49</sup>. Infere-se, assim, que os princípios dispostos nessa lei não excluem outras fontes do direito nacional<sup>50</sup>.

Portanto, devido à dinâmica de troca de informações entre as partes envolvidas proposta pelo *Open Banking*, estes métodos deverão ser seguros e eficientes para determinar se os dados

<sup>45</sup> “[...] 48% of negative discussions worldwide around Open Banking centered on consumers’ data protection and cybersecurity concerns. Consumer trust remains low or moderate in nine of the 10 markets we surveyed, irrespective of the regulatory environment.” (THOMAS; BELLENS; CLAUS, 2020).

<sup>46</sup> Com o desenvolvimento da tecnologia, passa a existir um novo conceito de privacidade, sendo o consentimento do interessado o ponto de referência de todo o sistema de tutela da privacidade, direito que toda pessoa tem de dispor com exclusividade sobre as próprias informações, nelas incluindo o direito à imagem [...] (STJ, REsp 1.168.547/RJ, 4.ª T.j. 11.05.2010, v.u., rel. Min. Luis Felipe Salomão, DJe 07.02.2011).

<sup>47</sup> LGPD: “Art. 58-A. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto de 23 (vinte e três) representantes, titulares e suplentes [...] essencialmente do executivo, legislativo, justiça, sociedade civil, tecnológica etc.” (BRASIL, 2018).

<sup>48</sup> Leia-se: órgãos de defesa do consumidor, conforme disposto no art. 55-K, parágrafo único (LGPD).

<sup>49</sup> “Art. 64. Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte” (BRASIL, 2018).

<sup>50</sup> O regime previsto pela LGPD não exclui aquele definido pelo CDC. “A incidência em comum dos arts. 7º do CDC e 64 da LGPD firmam a conclusão de que os direitos dos titulares dos dados previstos nas respectivas normas devem ser cumulados e compatibilizados pelo intérprete”. MIRAGEM, (2019a, p.177).

estão sendo fornecidos de fato para a entidade que foi autorizada pelo cliente. Ainda, não ocorra o respectivo vazamento de informações sensíveis e na eventualidade de ocorrer, qual parte será responsável pelo vazamento.

Com relação à **proteção de dados do usuário**, é importante demonstrar o tema do *Open Banking* com a proteção de dados, refletido assim na LGPD, onde as informações bancárias de cada pessoa devem ser tratadas como informações pessoais.

Joelsons (2020) destaca que, nos termos do art. 41 da LGPD, houve a indicação de um encarregado pelo tratamento de dados pessoais. Este profissional servirá de ligação entre a empresa e os respectivos titulares de dados, os controladores, e a ANPD. Também será o encarregado para coordenar os colaboradores sobre o *modus operandi* a serem praticados.

Afinal, todas as informações básicas do cliente estão lá (RG, CPF, endereço, filiação, renda, cadastro patrimonial, etc.). Logo, este perfil bancário em muito revela a privacidade da pessoa através do sigilo bancário vis-à-vis a sua intimidade e são bens jurídicos a serem tutelados. A proteção de dados pessoais e sua repercussão, no mercado de consumo, relaciona-se com a proteção da vida privada e da intimidade (MIRAGEM, 2019a).

O termo ou expressão "sigilo bancário" não está expressamente prevista na Constituição Federal. Por essa razão, Bellinetti (1996) prefere definir o sigilo bancário como a obrigação jurídica das instituições financeiras, organizações auxiliares (podemos aqui estender as *fintechs* neste contexto) e as pessoas então envolvidas de não revelarem as informações envolta da atividade bancária de cada cliente, salvo justa causa. Portanto, dados dessa natureza encontram abrigo no art. 5º. inciso X da constituição<sup>51</sup>.

Os contratos bancários resguardam sua proteção no sigilo bancário (LC 105/2001). Contudo, há hipóteses em que o sigilo poderá ser restrito conforme art. 1º § 3º, que trata das hipóteses em que não há violação<sup>52</sup>. Salienta-se que os bancos reciprocamente considerados, para efeitos do exercício do direito previsto conforme art. 1º, § 3º, I, não são considerados terceiros. E, onde as instituições financeiras poderão de acordo com a referida lei, compartilhar informações sigilosas, desde que haja o consentimento do cliente<sup>53</sup>.

Ainda, a Resolução nº 3.401/06, do BACEN, enfatiza no art. 3º que os bancos e instituições financeiras devem fornecer os dados, sempre que haja o consentimento do cliente<sup>54</sup>. Em paralelo, a LGPD reforça e obriga a clareza de que os dados sejam recolhidos ou tratados<sup>55</sup>,

<sup>51</sup> “[...] X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação (BRASIL, 1988).

<sup>52</sup> “Art.1 [...] § 3o Não constitui violação do dever de sigilo: I – a troca de informações entre instituições financeiras, para fins cadastrais, inclusive por intermédio de centrais de risco, observadas as normas baixadas pelo Conselho Monetário Nacional e pelo Banco Central do Brasil; II - o fornecimento de informações constantes de cadastro de emitentes de cheques sem provisão de fundos e de devedores inadimplentes, a entidades de proteção ao crédito, observadas as normas baixadas pelo Conselho Monetário Nacional e pelo Banco Central do Brasil; III – o fornecimento das informações de que trata o § 2o do art. 11 da Lei no 9.311, de 24 de outubro de 1996; IV – a comunicação, às autoridades competentes, da prática de ilícitos penais ou administrativos, abrangendo o fornecimento de informações sobre operações que envolvam recursos provenientes de qualquer prática criminosa; V – a revelação de informações sigilosas com o consentimento expresso dos interessados”. (BRASIL, 2001).

<sup>53</sup> “O consentimento faz com que não haja a ilicitude na comunicação de dados, a qual está pré-excluída pela vontade do interessado. Materialmente há comunicação de dados, mas juridicamente não existe violação ao sigilo pelo critério de que a inviolabilidade pode ser disposta por ato jurídico de vontade orientado ao assentimento. A possibilidade desse consentimento, aliás, está prevista expressamente na LC 105/01 1.º § 3.º, V”. (NERY JUNIOR, 2010).

<sup>54</sup> “Art. 3º As instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil devem fornecer a terceiros, quando formalmente autorizados por seus clientes, as informações cadastrais a eles relativas, de que trata a Resolução 2.835, de 30 de maio de 2001” (BANCO CENTRAL DO BRASIL, 2006).

<sup>55</sup> “Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular [...] Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular” (BRASIL, 2018).

conforme disposto nos art. 7º. e 8º., salvo disposições contrárias previstas na lei, por qualquer organização pública ou privada.

Desta maneira, o CDC assegurou para o consumidor seu direito irrestrito, imediato e gratuito às informações a seu respeito, bem como as fontes do registro e a identificação dos destinatários das informações então armazenadas. E devem guardar apenas informações verídicas e atuais.

Importante ainda, em relação aos arquivos de consumo negativos (“os negativados”), o dever de respeitar limites de acessibilidade dos dados, vedando o acesso de forma coletiva e massificada às informações arquivadas dada a natureza eminentemente particular dos dados armazenados nos arquivos de consumo, como é o caso, por exemplo, das informações sobre a inadimplência do consumidor. Nesta linha, os dados depreciadores então não podem permanecer armazenados em caráter perpétuo. O CDC é muito específico a este respeito, não permitindo prazo superior a cinco anos, ou quando prescrever ação de cobrança e débitos do consumidor (CARVALHO, 2003).

Conforme apurado acima, a preservação do sigilo dos dados bancários será um dos desafios do *Open Banking*. A lei do sigilo bancário, o CDC, LGPD por si só não serão de maneira determinante capazes de regulamentar as práticas do *Open Banking*. Assim, bancos, *fintechs*, e agentes estão obrigados ao silêncio. Uma vez o dado revelado fora deste contexto, acarretariam potencial dano ao cliente.

O *Open Banking* e o sigilo bancário tiveram novos entendimentos com o advento do cadastro positivo (lei 12.414/11, análoga ao cadastro negativo) que se dedica a notificar quanto ao adimplemento das obrigações assumidas por aqueles que, por livre e espontânea vontade, se dispuseram a se cadastrar no banco de dados. A partir da consulta ao banco de dados do cadastro positivo, a confiabilidade dos potenciais tomadores de crédito aumenta com bons apontamentos [...] <sup>56</sup>.

Para Bioni, um dos escritores (MACHADO; ORTELLADO; RIBEIRO, 2015, p. 46), o cadastro positivo estabelecia inicialmente a utilização do sistema *opt-in*, que, segundo o autor, necessita do *de acordo* do titular das informações pessoais para que haja acesso e tratamento dos dados. Porém, a LC 166/2019 trouxe a possibilidade de ser pelo sistema *opt-out*, que não necessita o consentimento prévio (BRASIL, 2019, *online*). Conforme a referida lei complementar (art. 4º., § 4º.), a comunicação ao cadastrado/titular deverá ocorrer em até 30 dias e informar de maneira clara e objetiva quais são os canais de comunicação para manifestação de discordância.

Ao seguir sua estrutura baseada no CDC e na LGPD, o *Open Banking* parte da premissa de que toda a informação e cedência de dados devem ocorrer somente com o consentimento do cliente. Contudo, a lei complementar destacada poderá trazer futuras inseguranças ao *Open Banking* em seu cunho jurídico. Principalmente quanto ao prévio consentimento referido, uma vez que a mesma alterou a legislação prévia, liberando o intercâmbio de dados “positivos” do usuário, e, portanto, não constituindo violação ao dever de sigilo neste quesito <sup>57</sup>.

Outro ponto relevante trata-se dos **riscos cibernéticos**. Em levantamento entre diversos conselheiros de grandes empresas, em relação aos serviços financeiros, uma das principais ameaças no seu entender recaem sobre os riscos cibernéticos. Com a ampliação dos canais

---

<sup>56</sup> Com isso, os credores podem saber o tipo e o tamanho do risco em jogo, o que possibilita o ajuste de suas taxas de juros e a oferta de um maior elastério aos prazos para pagamento das dívidas de acordo com a extensão desses riscos. Diante disso, pessoas físicas e jurídicas optam pela inclusão no cadastro positivo com a pretensão de constarem em um banco de dados que pode elencá-las como boas pagadoras (PORTO, FRANCO 2018).

<sup>57</sup> Na Lei Complementar 166/2019 deliberou-se, pela ampla liberação do acesso às anotações financeiras de todos os indivíduos [...]. As instituições financeiras podem fornecer, a gestores de bancos de dados, informações relativas a operações de crédito, ativas e passivas, e obrigações de Cadastros Positivos de Crédito [...]. Não mais constitui violação ao dever de sigilo por parte das mencionadas entidades tal atividade, consoante dispõe o seu art. 1º, § 3º, inciso VII (SILVA, 2019).

digitais e as soluções envolta do *Open Banking*, problemas relacionados a este tema se tornaram ainda mais complexos sendo que os principais fatores relacionados são o de vazamento, uso indevido ou perda de dados (CASTRO; CAJAZEIRA, 2018).

O *Open Banking* impactará o gerenciamento de riscos de fraude de várias maneiras, pois contará com a segurança de terceiros para proteger as informações bancárias dos clientes (por meio das APIs). Se estes terceiros não fornecerem proteção adequada, os clientes provavelmente considerarão o banco como respectivos culpados (KPMG, 2019).

Diante desse contexto de novas tecnologias no setor financeiro e a crescente interação entre os sistemas tecnológicos das instituições financeiras e de outros parceiros comerciais, o próprio BACEN, em sua circular 3.909/2018, aborda a implantação da política de segurança cibernética, onde trata de três grandes temas no seu texto: (i) política de segurança cibernética; (ii) contratação de serviços de processamento e armazenamento de dados e de computação em nuvem onde as políticas cibernéticas implementadas pelas instituições devem assim buscar assegurar confidencialidade, a integridade e a disponibilidade dos sistemas de informação utilizados (art. 2º, caput)<sup>58</sup>. Logo, trata-se de uma norma de caráter preventivo e voltada ao controle dos riscos das instituições credenciadas bem como das respectivas políticas cibernéticas; e, (iii) integração da proteção de dados pessoais com regras de segurança da informação.

A LGPD, em seu escopo geral, elenca cinco espécies de potenciais infrações, tais como acesso não autorizado, destruição de dados, perda de dados, alteração de dados, e qualquer forma de tratamento inadequado ou ilícito dos mesmos. Para Schwartzman (2020), a fim de dirimir as infrações elencadas, conforme a circular 3.909/2018, os destaques estão no art. 3º. da referida circular<sup>59</sup> como mecanismos de rastreabilidade, ou seja, registro das operações realizadas na cadeia de informação, alinhado a LGPD (controle que seja auditável). Deverá também ocorrer classificação quanto a sua relevância. Logo, quanto maior a criticidade, maiores os procedimentos de segurança e controle em geral.

Outro ponto aplicável à segurança cibernética é o dever de elaboração de cenários de incidentes devendo as instituições de pagamento realizarem testes periódicos dos procedimentos nele previstos, baseados em cenários de ocorrência de incidentes. E, para reduzir potenciais vulnerabilidades das instituições participantes no quesito segurança cibernética, elencou também a determinação de procedimentos mínimos conforme (Art. 3º, § 2º)<sup>60</sup>. Destacam-se aqui a adoção de criptografia e exigência de varredura contra *softwares* maliciosos, periodicamente, e estabelecimento de mecanismos de rastreabilidade.

O objetivo do *Open Banking* é a linguagem uniforme para o uso em geral de bancos, *fintechs* e clientes em geral. Fatores esses somente permitidos pelo advento do avanço tecnológico. Porém, este ambiente tornou-se, em contrapartida, propício e vulnerável, atraindo potencial de riscos cibernéticos através de fraudes eletrônicas em geral.

<sup>58</sup> “Art. 2º As instituições de pagamento devem implementar e manter política de segurança cibernética formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados” (BANCO CENTRAL DO BRASIL, 2018a).

<sup>59</sup> “Art. 3º A política de segurança cibernética deve contemplar, no mínimo [...] III - os controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis; V - as diretrizes para: c) a classificação dos dados e das informações quanto à relevância; e VI - os mecanismos para disseminação da cultura de segurança cibernética na instituição, incluindo: [...] b) a prestação de informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros” (BANCO CENTRAL DO BRASIL, 2018a).

<sup>60</sup> “[...] § 2º Os procedimentos e os controles de que trata o inciso II do caput devem abranger a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações” (BRASIL, 2018).



As relações jurídicas existentes entre estes atores mencionados no *Open Banking*, em razão inclusive da atividade desenvolvida e de sua natureza monetária, vão além dos esforços irrestritos em prestar a melhor informação ao cliente. Devem resguardar todos na mais absoluta confiança e desenvolver modelos seguros a fim de possibilitar a identificação de quem encaminhou ou transmitiu os dados. Assim como, elencar a finalidade e seu local de destino, pois será ponto crucial a fim de evitar a violação das informações e acesso não autorizado.

**Outro ponto de atenção é a responsabilidade por danos.** O *Open Banking* possui, entre suas principais premissas, o resguardo e proteção dos dados pessoais. Em caso de violação, deverão, portanto, ser observadas as regras de responsabilidade estabelecidas na LGPD.

É importante compreender que para evitar danos causados pelo tratamento incorreto de dados pessoais, deva existir uma obrigação de segurança tanto aos operadores quanto aos controladores de dados por tratar-se de atividade de cunho profissional e que estes, de antemão, possuam profissionalismo e conhecimento para resguardar a integridade das informações e privacidade dos titulares (MIRAGEM, 2019a).

No ordenamento jurídico brasileiro, existem tanto atividades financeiras exercidas pelo Estado, como também aquelas realizadas pelas instituições financeiras e bancárias. Em face dessa característica, as fontes normativas sobre a responsabilidade civil nos contratos bancários decorrem do Código Civil e do Código de Defesa do Consumidor, além das normas de direito bancário e as resoluções propostas pelo Banco Central.

A responsabilidade civil tem função de destaque na disciplina de proteção de dados pessoais, principalmente se houver a definição de casos específicos de responsabilidade objetiva. Importante considerar a imensa dificuldade de caracterizar o dano, vide este ser um dos problemas centrais enfrentados pela consolidação da tutela da privacidade (DONEDA, 2007). Assim, poderá ensejar, em caso de tratamento indevido, pretensão de reparação aos titulares dos dados por danos tanto de esfera patrimonial e moral como individual ou coletivo (MIRAGEM, 2019a).

Na LGPD, a responsabilidade civil surge a partir do art. 42<sup>61</sup>, onde estabelece que o controlador e operador de dados, no exercício de suas atividades de tratamento, serão obrigados à reparação do dano durante o exercício da atividade de tratamento dos dados pessoais (MENDES; DONEDA, 2018; MIRAGEM, 2019a). No § 1º do mesmo artigo, confere-se a responsabilidade solidária, gerando um efeito dominó nas partes envolvidas, refletindo conjuntamente as empresas responsáveis pela cessão dos dados (ANDRÉA; ARQUITE; CAMARGO, 2020).

Ou seja, os agentes de tratamento respondem solidariamente (tanto operador e controlador) ou no caso de haver dois controladores, por exemplo. Ainda, o operador responderá de maneira solidária se inadimplir as obrigações definidas na LGPD ou não houver respeitado as instruções do controlador. Conforme Miragem (2019a) é a “*hipótese em que o operador se equipara ao controlador*” vide (art. 42, §1º, I). Destaca-se, portanto, que estas são as duas únicas hipóteses previstas de solidariedade (MENDES; DONEDA, 2018).

Caso os controladores estiverem “diretamente envolvidos” no tratamento que resultem danos ao titular dos dados, também responderão solidariamente pela reparação (art. 42, §1º, II).

---

<sup>61</sup> “Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. § 1º A fim de assegurar a efetiva indenização ao titular dos dados: I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei; II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.” [...] (BRASIL, 2018).

Já o art. 42, § 2º da LGPD, confere a imputação de responsabilidade, incluindo a premissa de inversão do ônus da prova em favor do titular dos dados, tendo os mesmos abrigos da hipossuficiência do cliente como os do campo das relações de consumo (MIRAGEM, 2019a).

Infere-se a isso, deste modo, as causas de dano patrimonial, moral, individual ou coletivo, assim como eventual omissão, e por consequência não adotarem as medidas cabíveis e esperadas de segurança previstas em legislação, dando causa aos danos.

Para conseguir garantir uma indenização efetiva pelo titular, o operador dos dados irá responder solidariamente aos danos causados, quando descumprir as obrigações postas em lei ou ainda se não houver seguido as instruções lícitas do controlador. Porém, a lei prevê excludentes de responsabilidade em seu art. 43. A questão está no caput<sup>62</sup>, onde diz expressamente que “os agentes de tratamento só não serão responsabilizados quando provarem [...]” (MENDES; DONEDA, 2018; DIVINO; LIMA, 2020).

A LGPD considera que o tratamento de dados pessoais será considerado irregular no que tange aos atos ilícitos praticados pelos particulares. Deve-se tratar assim, como responsabilidade objetiva, conforme expressa o art. 43 as hipóteses em que não serão responsabilizados conforme as situações ali descritas (DIVINO; LIMA, 2020). Pelas práticas atuais, as evidências e provas referidas deverão ser técnicas e baseadas nos protocolos já existentes de tecnologia da informação presentes.

Ainda sobre a questão, infere-se do art. 44, assim como ocorre conforme responsabilidade do fornecedor no CDC, que serão considerados irregulares, os dados que não respeitarem o devido nível de segurança. Aqueles, portanto, que são esperados com as tecnologias disponíveis no momento<sup>63</sup>. Se houver danos em decorrência dessa desobediência tanto controlador como operador, serão responsabilizados<sup>64</sup>.

A LGPD, no tocante às hipóteses de violação que inferirem nas relações de consumo, permanecem na discricionariedade do CDC. Conforme já preceituado, nas situações jurídicas onde o CDC carregar uma melhor resolução a situação ilícita, restringe-se a esse normativo. Por outro lado, onde a lei de proteção de dados oferecer uma proteção de grau equivalente ou maior deve-se aplicar o diálogo das fontes (DIVINO; LIMA, 2020).

Assim, dos danos gerados pelo tratamento indevido de dados, o art. 45 da LGPD, conduz ao fato de dano no serviço, e traz os preceitos em linha com o art. 14 do CDC. O artigo diz que o fornecedor de serviços, independentemente da existência de culpa responde pela reparação dos danos que forem causados aos consumidores por defeitos relativos à prestação dos serviços (BRASIL, 1990).

Em analogia ao *Open Banking*, o artigo esclarece, portanto, que se o serviço prestado pela instituição financeira causar dano, e como fornecedora não puder oferecer a segurança, resta evidenciado problema no serviço bancário ou financeiro. Diz Marques (2001): “*Neste caso, haverá um risco profissional do banco, se estes softwares e hardwares não funcionarem adequadamente e com o grau de segurança deles esperados*”.

---

<sup>62</sup> “Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem: I - que não realizaram o tratamento de dados pessoais que lhes é atribuído; II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro” (BRASIL, 2018).

<sup>63</sup> “Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado” (BRASIL, 2018).

<sup>64</sup> “[...] trata-se de situar, em relação à responsabilidade pelos danos causados em relação ao tratamento indevido de dados, qual o lugar dos riscos do desenvolvimento, considerando, neste caso, a própria previsibilidade de uma atualização e avanço técnico em atividades vinculadas à tecnologia da informação, mais veloz do que em outras atividades econômicas [...]” (MIRAGEM, 2019a).

Outro efeito é a submissão de eventuais pretensões de reparação pelos consumidores ao prazo prescricional de cinco anos do conhecimento do dano conforme o art. 27 do CDC (MIRAGEM, 2019a).

Em decorrência do exposto, no intuito de afastar eventuais responsabilidades em relação aos dados compartilhados, as instituições financeiras, bancos e *fintechs* envolvidos no processo precisarão se precaver a fim de certificar e comprovar que passaram de fato os dados apenas para as partes autorizadas e que na transmissão não houve vazamento de dados. Se este contexto for preenchido, não poderiam, assim, as mesmas serem as responsabilizadas, pois não estariam mais na relação de consumo onde ocorreu o erro ou fato. Isto poderá ser um fator essencial do *Open Banking* no Brasil para sua consolidação e confiabilidade.

#### 4 CONSIDERAÇÕES FINAIS

1. O sistema tem o objetivo de proporcionar a criação de um ambiente mais aberto e competitivo entre as instituições financeiras e as chamadas *fintechs*;
2. A ideia central é que o *Open Banking* seja uma plataforma onde os dados sobre clientes, produtos e serviços fluam no sistema financeiro de maneira padronizada;
3. As questões inerentes ao *Open Banking* devem, hoje, ser lidas e interpretadas em harmonia com os princípios consagrados no CDC como boa-fé e transparência;
4. O dever de informação torna-se ainda mais imperioso para a proteção na escolha onde o consumidor possui o direito de livre escolha e de liberdade na aquisição de serviços financeiros;
5. O *Open Banking*, então, parte do princípio de que os dados pessoais e as informações bancárias dos clientes pertencem a estes sujeitos, e não às instituições financeiras, alinhado às premissas da LGPD;
6. Os contratos bancários resguardam sua proteção no sigilo bancário (LC 105/2001). Em paralelo, a LGPD reforça e obriga a clareza de que os dados sejam recolhidos ou tratados;
7. A lei complementar 166/2019 poderá trazer futuras inseguranças ao *Open Banking* em seu cunho jurídico. Principalmente quanto ao prévio consentimento referido;
8. A LGPD, em seu escopo geral, elenca cinco espécies de potenciais infrações, para dirimir há previsão de mecanismos de rastreabilidade (controle que seja auditável), e quanto maior a criticidade, maiores os procedimentos de segurança e controle em geral;
9. Este ambiente tornou-se, em contrapartida, propício e vulnerável, atraindo potencial de riscos cibernéticos através de fraudes eletrônicas em geral;
10. No *Open Banking*, em razão inclusive da atividade desenvolvida e de sua natureza monetária, as obrigações vão além dos esforços irrestritos em prestar a melhor informação ao cliente;
11. Importante considerar a imensa dificuldade de caracterizar o dano. Assim os agentes de tratamento respondem solidariamente (tanto operador e controlador);
12. Em analogia se o serviço prestado pela instituição financeira causar dano, e como fornecedora não puder oferecer a segurança, resta evidenciado problema no serviço bancário ou financeiro;
13. Em decorrência do exposto, no intuito de afastar eventuais responsabilidades em relação aos dados compartilhados, as instituições envolvidas precisarão se precaver a fim de certificar e comprovar que passaram de fato os dados apenas para as partes autorizadas e que na transmissão não houve vazamento de dados;
14. Se este contexto for preenchido, não poderiam, assim, as mesmas serem as responsabilizadas, pois não estariam mais na relação de consumo onde ocorreu o erro ou

fato. Isto poderá ser um fator essencial do *Open Banking* no Brasil para sua consolidação e confiabilidade.

## REFERÊNCIAS BIBLIOGRÁFICAS

ANDRÉA, Gianfranco Faggin Mastro; ARQUITE, Higor Roberto Leite; CAMARGO, Juliana Moreira. Proteção dos dados pessoais como direito fundamental: a evolução da tecnologia da informação e a lei geral de proteção de dados no Brasil. **Revista de Direito Constitucional e Internacional**, São Paulo, v. 28, n. 121, p. 115-139, set./out. 2020.

BANCO CENTRAL DO BRASIL. **Open Banking**: o que é? [Brasília]: Banco Central do Brasil, [2021a?]. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/openbanking>. Acesso em: 21 ago. 2021.

BANCO CENTRAL DO BRASIL. **Regulação prudencial**. [Brasília]: Banco Central do Brasil, [2021b]. *Online*. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/regprudencialsegmentacao>. Acesso em: 18 ago. 2021.

BANCO CENTRAL DO BRASIL. **[Agenda] BC#**. [Brasília]: Banco Central do Brasil, [2020a?]. Disponível em: <https://www.bcb.gov.br/acessoinformacao/bchashtag>. Acesso em: 06 set. 2021.

BANCO CENTRAL DO BRASIL. **Agenda BC#**: uma pauta para o sistema financeiro do futuro. [Brasília]: Banco Central do Brasil, 2020b. Disponível em: [https://www.bcb.gov.br/conteudo/home-ptbr/TextosApresentacoes/ppt\\_balanco\\_agenda\\_bc\\_2019.pdf](https://www.bcb.gov.br/conteudo/home-ptbr/TextosApresentacoes/ppt_balanco_agenda_bc_2019.pdf). Acesso em: 17 ago. 2021.

BANCO CENTRAL DO BRASIL. **Resolução conjunta nº 1, de 4 de maio de 2020**. Dispõe sobre a implementação do Sistema Financeiro Aberto (*Open Banking*). [Brasília]: Banco Central do Brasil, 2020c. Disponível em: [https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/51028/Res\\_Conj\\_0001\\_v3\\_P.pdf](https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/51028/Res_Conj_0001_v3_P.pdf). Acesso em: 19 set. 2021.

BANCO CENTRAL DO BRASIL. **Circular nº 3.909, de 16 de agosto de 2018**. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e [...]. [Brasília]: Banco Central do Brasil, 2018a. Disponível em: [https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50645/Circ\\_3909\\_v1\\_O.pdf](https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50645/Circ_3909_v1_O.pdf). Acesso em: 23 ago. 2021.

BANCO CENTRAL DO BRASIL. **Resolução nº 4.656, de 26 de abril de 2018**. Dispõe sobre a sociedade de crédito direto e a sociedade de empréstimo entre pessoas, disciplina a realização de operações de empréstimo [...]. [Brasília]: Banco Central do Brasil, 2018b. Disponível em: [https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50579/Res\\_4656\\_v1\\_O.pdf](https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50579/Res_4656_v1_O.pdf). Acesso em: 23 ago. 2021.

BANCO CENTRAL DO BRASIL. **Resolução nº 3401**. Dispõe sobre a quitação antecipada de operações de crédito e de arrendamento mercantil, a cobrança de tarifas nessas operações, bem como sobre a obrigatoriedade de fornecimento de informações cadastrais. Brasília: Banco

Central do Brasil, 2006. Disponível em: [https://www.bcb.gov.br/pre/normativos/res/2006/pdf/res\\_3401\\_v2\\_p.pdf](https://www.bcb.gov.br/pre/normativos/res/2006/pdf/res_3401_v2_p.pdf). Acesso em: 22 ago. 2021.

BANK OF ENGLAND. **Open data for SME finance**: what we proposed and what we have learnt. [London]: Bank of England, 2020. *E-book*. Disponível em: <https://www.bankofengland.co.uk/-/media/boe/files/fintech/open-data-for-sme-finance.pdf?la=en&hash=FD4BC43BBD61EDEC5F8460C6BB7488EFDE647581>. Acesso em: 28 ago. 2021.

BANK OF INTERNATIONAL SETTLEMENTS (BIS). **Basel committee on banking supervision**: report on Open Banking and application programming interfaces. [Basel, Suíça]: BIS, 2019. *E-book*. Disponível em: <https://www.bis.org/bcbs/publ/d486.pdf>. Acesso em: 26 ago. 2021.

BELLINETTI, Luiz Fernando. Limitações legais ao sigilo bancário. **Revista de Direito do Consumidor**, São Paulo, v. 18, p. 141-161, abr./jun. 1996.

BRASIL. **Constituição da República Federativa do Brasil**, de 05.10.1988. Brasília, 1988. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 10 nov. 2021.

BRASIL. **Lei Complementar nº105, de 10 de janeiro de 2001**. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Brasília: Presidência da República, 2001. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/lcp/lcp105.htm](http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm). Acesso em: 10 nov. 2021.

BRASIL. **Lei Complementar nº 166, de 8 de abril de 2019**. Altera a Lei Complementar nº 105, de 10 de janeiro de 2001, e a Lei nº 12.414, de 9 de junho de 2011, para dispor sobre os cadastros positivos de crédito e regular a responsabilidade civil dos operadores. Brasília: Presidência da República, 2019. *Online*. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/lcp/Lcp166.htm](http://www.planalto.gov.br/ccivil_03/leis/lcp/Lcp166.htm). Acesso em: 16 set. 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, 2018. *Online*. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/L13709compilado.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm). Acesso em: 16 set. 2021.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília: Presidência da República, 1990. *Online*. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/l8078compilado.htm](http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm). Acesso em: 19 set. 2021.

BROLLO, Gustavo Deucher; ALMEIDA, Marcus Elidius Michelli de. *Open Banking* e sua recente regulamentação no Brasil. **Revista de Direito Bancário e do Mercado de Capitais**, [S. l.], v. 89, p. 193-212, jul./set. 2020.

CARR, Brad; URBIOLA, Pablo; DELLE-CASE, Adrien. **Liability and consumer protection in Open Banking**. [S. l.]: Institute of International Finance, 2018. *E-book*. Disponível em: [https://www.iif.com/portals/0/Files/private/32370132\\_liability\\_and\\_consumer\\_protection\\_in\\_open\\_banking\\_091818.pdf](https://www.iif.com/portals/0/Files/private/32370132_liability_and_consumer_protection_in_open_banking_091818.pdf). Acesso em: 18 ago. 2021.

CARVALHO, Ana Paula Gambogi. O consumidor e o direito à autodeterminação informacional: considerações sobre os bancos de dados eletrônicos. **Revista de Direito do Consumidor**, São Paulo, v. 46, p. 77-119, abr./jun. 2003.

CASTRO, Marco; CAJAZEIRA, Fábio. **Como lidar com a supervisão de riscos cibernéticos?** [S. l.]: PwC, 2018. *E-book*. Disponível em: [https://www.pwc.com.br/pt/estudos/preocupacoes-ceos/mais-temas/2018/risco\\_ciber\\_gov\\_2018.pdf](https://www.pwc.com.br/pt/estudos/preocupacoes-ceos/mais-temas/2018/risco_ciber_gov_2018.pdf). Acesso em: 19 set. 2021.

DIVINO, Sthéfano Bruno Santos; LIMA, Taisa Maria Macena de. Responsabilidade civil na lei geral de proteção de dados brasileira. **Revista Em Tempo**, [S. l.], v. 20, n. 1, nov. 2020. Disponível em: <https://revista.univem.edu.br/emtempo/article/view/3229>. Acesso em: 15 set. 2021.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, SC, v. 12, n. 2, p. 91-108, jul./dez. 2011.

DONEDA, Danilo. A tutela da privacidade no Código Civil de 2002. [ÂNIMA: **Revista eletrônica do Curso de Direito Opet**, Curitiba], v. 1, p. [1-10], [2007?]. Disponível em: [https://www.opet.com.br/faculdade/revista-anima/pdf/anima1/artigo\\_Danilo\\_Doneda\\_a\\_tutela.pdf](https://www.opet.com.br/faculdade/revista-anima/pdf/anima1/artigo_Danilo_Doneda_a_tutela.pdf). Acesso em: 11 out. 2021.

THE EUROPEAN PARLIAMENT; THE COUNCIL OF THE EUROPEAN UNION. Directive (EU) 2015/2366 of the Parliament and the Council. **Official Journal of the European Union**. [Luxemburgo], dez. 2015. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=PT>. Acesso em: 23 ago. 2021.

FEBRABAN. **Pesquisa FEBRABAN de tecnologia bancária 2019**. [S. l.]: Deloitte, 2019. *E-book*. Disponível em: <https://cmsarquivos.febraban.org.br/Arquivos/documentos/PDF/Pesquisa-FEBRABAN-Tecnologia-Bancaria-2019.pdf>. Acesso em: 17 ago. 2021.

FRAZÃO, Ana. **Economia do compartilhamento e tecnologias disruptivas**: a compreensão dos referidos fenômenos e suas consequências sobre a regulação jurídica. [Brasília]: Ana Frazão, 2017. Disponível em: [http://www.professoraanafrazao.com.br/files/publicacoes/2017-06-14-Economia\\_do\\_compartilhamento\\_e\\_tecnologias\\_disruptivas.pdf](http://www.professoraanafrazao.com.br/files/publicacoes/2017-06-14-Economia_do_compartilhamento_e_tecnologias_disruptivas.pdf). Acesso em: 05 set. 2021.

GOETTENAUER, Carlos. *Open Banking* e teorias de regulação da *Internet*. **Revista de Direito Bancário e do Mercado de Capitais**, [S. l.], v. 82, p. 109-128, out./dez. 2018.

INTERNETLAB PESQUISA EM DIREITO E TECNOLOGIA. **O que está em jogo no debate sobre dados pessoais no Brasil?**: relatório final sobre o debate público promovido pelo Ministério da Justiça sobre o Anteprojeto de Lei de Proteção de Dados Pessoais. São Paulo: INTERNETLAB, 2016. *E-book*. Disponível em: [internetlab.org.br/wp-content/uploads/2016/05/reporta\\_apl\\_dados\\_pessoais\\_final.pdf](http://internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf). Acesso em: 06 set. 2021.

JOAQUIM, Gustavo; DOORNIK, Bernardus Van; ORNELAS, José Renato. Bank competition, cost of credit and economic activity: evidence from Brazil. Banco Central do

Brasil. **Working Paper Series**, Brasília, n. 508, out. 2019, atual. maio 2020. Disponível em: <https://www.bcb.gov.br/pec/wps/ingl/wps508.pdf>. Acesso em: 18 ago. 2021.

JOELSONS, Marcela. Lei geral de proteção de dados em vigor: impactos imediatos e possíveis desafios à luz da experiência da União Europeia, **Revista dos Tribunais**, São Paulo, n. 1022, p. 175-194, dez. 2020.

KPMG. **Pesquisa global sobre fraude bancária**: a ameaça multifacetada da fraude: os bancos estão prontos para enfrentar este desafio? [S. l.]: KPMG, 2019. *E-book*. Disponível em: <https://assets.kpmg/content/dam/kpmg/br/pdf/2021/07/pesquisa-global-fraude-bancaria.pdf>. Acesso em: 9 set. 2021.

MACHADO, Jorge A. S.; ORTELLADO, Pablo; RIBEIRO, Márcio Moretto. (coord.). **Xequemate**: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil. São Paulo: GPoPAI/USP, 2015.

MARQUES, Cláudia Lima. Proteção do consumidor no comércio eletrônico e a chamada nova crise do contrato: por um direito do consumidor aprofundado. **Revista de Direito do Consumidor**, São Paulo, v. 57, p. 9-59, jan./mar. 2006.

MARQUES, Cláudia Lima. Sociedade de informação e serviços bancários: primeiras observações. **Revista de Direito do Consumidor**, São Paulo, v. 39, p. 49-74, jul./set. 2001.

MARTELLO, Alexandre. Indicado para o Banco Central defende autonomia da instituição em sabatina no Senado. **G1: Economia**, Brasília, 2019. *Online*. Disponível em: <https://g1.globo.com/economia/noticia/2019/02/26/indicado-para-chefiar-bc-campos-neto-defende-autonomia-da-instituicao-e-reducao-do-estado.ghtml>. Acesso em: 19 ago. 2021.

MARTINS, Marcelo. **O que são pagamentos instantâneos?** São Paulo: Blockchain Academy, 2019. *Online*. Disponível em: <https://blockchainacademy.com.br/blog/negocios/o-que-sao-pagamentos-instantaneos/>. Acesso em: 19 ago. 2021.

MENDES, Laura Schertel; BIONI, Bruno R. O regulamento europeu de proteção de dados pessoais e a Lei Geral de Proteção de Dados brasileira: mapeando convergências na direção de um nível de equivalência. **Revista de Direito do Consumidor**, São Paulo, ano 28, v. 124, p. 157-180, jul./ago. 2019.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, São Paulo, ano 27, v. 120, p. 469-483, nov./dez. 2018.

MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (lei 13.709/2018) e o direito do consumidor. **Revista dos Tribunais**, São Paulo, v. 1009, p. 173-222, nov. 2019a.

MIRAGEM, Bruno. Novo paradigma tecnológico, mercado de consumo digital e o direito do consumidor **Revista de Direito do Consumidor**, São Paulo, ano 28, v. 125, p. 17-62, set./out. 2019b.

MÜLLER, Bianca Abbott. Concorrência bancária no Brasil. **Revista de Direito Bancário e do Mercado de Capitais**, [S. l.], v. 30, p. 65-95, out./dez. 2005.

NERY JUNIOR, Nelson. Sigilo bancário: compartilhamento FEBRABAN-SERASA. *In*: NERY JUNIOR, Nelson. **Soluções práticas – Nery**. São Paulo: Revista dos Tribunais, 2010. p. 443-489. v. 1.

OPEN BANKING BRASIL. **Conheça o Open Banking**. [S. l.]: *Open Banking*, [2021]. *Online*. Disponível em: <https://openbankingbrasil.org.br/conheca-o-open-banking/>. Acesso em: 19 ago. 2021.

PASQUAL, Cristina S.; PACHECO, Thaise M. N. D. *Fintechs: (r)evolução tecnológica no mercado financeiro e os reflexos nas relações de consumo*. *In*: ENCONTRO INTERNACIONAL DO CONPEDI, 10., 2019, Valência, ES. [Anais]. Valência, ES: CONPEDI, 2019. p. 189-207. Disponível em: <http://site.conpedi.org.br/publicacoes/150a22r2/rb8x03d1/WJ74ZfyY1LV7V8rI.pdf>. Acesso em: 06 set. 2021.

PORTO, Antonio José Maristrello, FRANCO, Paulo Fernando de Mello. Por uma análise também econômica da responsabilidade civil do cadastro positivo: abordagem crítica do art. 16 da Lei 12.414/2011. **Revista de Direito do Consumidor**, São Paulo, v. 115, p. 247-271, jan./fev. 2018.

REDAÇÃO NUBANK. **O que é fintech e por que esse termo ficou tão popular?**: empresas oferecem soluções mais simples e baratas para a população. São Paulo: Nubank, 2020. *Online*. Disponível em: <https://blog.nubank.com.br/fintech-o-que-e/>. Acesso em: 27 ago. 2021.

RIBEIRO, Alexandre O.; BAGNOLI, Vicente. *Open Banking: impactos e desafios no mercado financeiro*. **Revista da Academia Brasileira de Direito Constitucional**, Curitiba, v. 13, n. 23, p. 216-242, ago./dez. 2020.

ROBINSON, Alex. Will Open Banking lead to the next wave of the UK's fraud epidemic? **Finextra**, Londres, maio 2021. *Online*. Disponível em: <https://www.finextra.com/blogposting/20294/will-open-banking-lead-to-the-next-wave-of-the-uks-fraud-epidemic>. Acesso em: 24 ago. 2021.

SCHUR, Rafael. **Por que construir a confiança do consumidor é a chave para o sucesso do Open Banking no Brasil?** [S. l.]: EY, 2019. *Online*. Disponível em: [https://www.ey.com/pt\\_br/banking-capital-markets/why-building-consumer-trust-is-key-to-brazil-open-banking-success](https://www.ey.com/pt_br/banking-capital-markets/why-building-consumer-trust-is-key-to-brazil-open-banking-success). Acesso em: 16 set. 2021.

SCHWARTZMAN, Felipe. Lei Geral de Proteção de Dados Pessoais e riscos cibernéticos: coexistência de normas no mercado de meios de pagamento. *In*: COHEN, Gabriel (coord.). **Direitos dos meios de pagamento: natureza jurídica e reflexões sobre lei nº 12.865/2013**. São Paulo: Editora Quartier Latin, 2020. p. 379-421.

SILVA, Joseane Suzart Lopes da. Cadastros positivos de crédito: as inovações arregimentadas pela lei complementar 166/2019 e a fundamental proteção dos vulneráveis pelo sistema nacional de defesa do consumidor. **Revista de Direito do Consumidor**, São Paulo, ano 28, v. 126, p. 135-177, nov./dez. 2019.



TAIAR, Estevão. *Open Banking* terá autorregulação assistida pelo BC, diz diretor. **Valor econômico: Finanças**, Brasília, 2020. *Online*. Disponível em: <https://valor.globo.com/financas/noticia/2020/06/29/open-banking-tera-autorregulacao-assistida-pelo-bc-diz-diretor.ghtml>. Acesso em: 18 ago. 2021.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **A Lei Geral de Proteção de Dados Pessoais**: e suas repercussões no direito brasileiro. São Paulo: Thomson Reuters: Revista dos Tribunais, 2019.

THOMAS, Hamish; BELLENS, Jan; CLAUS, Kai-Christian. **EY Open Banking opportunity index**: where Open Banking is set to thrive. [S. l.]: EY, 2020. *Online*. Disponível em: [https://www.ey.com/en\\_gl/banking-capital-markets/ey-open-banking-opportunity-index-where-open-banking-is-set-to-thrive](https://www.ey.com/en_gl/banking-capital-markets/ey-open-banking-opportunity-index-where-open-banking-is-set-to-thrive). Acesso em: 04 set. 2021.

UNITED KINGDOM. **C.M.A**: Competition & Market Authority. [London]: C.M.A, [2021?]. Informações gerais do Departamento. *Online*. Disponível em: <https://www.gov.uk/government/organisations/competition-and-markets-authority>. Acesso: em 13 set. 2021.

WINTER, Estefano Luís de Sá. O novo ecossistema de serviços financeiros. **Revista Rumos**, [Rio de Janeiro], n. 292, p. 32-33, mar./abr. 2017.



Pontifícia Universidade Católica do Rio Grande do Sul  
Pró-Reitoria de Graduação  
Av. Ipiranga, 6681 - Prédio 1 - 3º. andar  
Porto Alegre - RS - Brasil  
Fone: (51) 3320-3500 - Fax: (51) 3339-1564  
E-mail: [prograd@pucrs.br](mailto:prograd@pucrs.br)  
Site: [www.pucrs.br](http://www.pucrs.br)