UNIVERSIDADE CATÓLICA DO SALVADOR
GRADUAÇÃO EM DIREITO

KARINA SILVA CALDEIRA CARVALHO

A APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS NAS INSTITUIÇÕES FINANCEIRAS: O MAPEAMENTO DAS DIFICULDADES EM FACE DA IMPLEMENTAÇÃO DO PROJETO OPEN BANKING

Salvador
2023

KARINA SILVA CALDEIRA CARVALHO

A APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS NAS INSTITUIÇÕES FINANCEIRAS: O MAPEAMENTO DAS DIFICULDADES EM FACE DA IMPLEMENTAÇÃO DO PROJETO OPEN BANKING

Artigo apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Universidade Católica do Salvador.

Orientador: Prof. Ms. Carlos Alberto José Barbosa Coutinho

Salvador
2023

A APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS NAS INSTITUIÇÕES FINANCEIRAS: O MAPEAMENTO DAS DIFICULDADES EM FACE DA IMPLEMENTAÇÃO DO PROJETO OPEN BANKING

Karina Silva Caldeira Carvalho[1]

Orientador: Prof. Me. Carlos Alberto José Barbosa Coutinho[2]

RESUMO: O presente artigo tem como objetivo identificar a responsabilidade civil das instituições financeiras perante o cliente em situações em que os seus dados não sejam coletados, tratados e transmitidos conforme as diretrizes da Lei Geral de Proteção de Dados, em face a implementação do Sistema Open Banking. Além de apresentar quais os mecanismos que podem ser sugeridos visando evitar ou atenuar a responsabilidade civil dessas instituições perante a violação da Lei geral de Proteção de Dados. Em primeiro plano, são apresentadas, as duas regulações; a LGPD e o Sistema Open Banking e os seus impactos sobre a proteção de dados dos clientes. Por fim, com vistas a contextualizar a controvérsia que permeia a respeito da responsabilidade civil das instituições financeiras diante a violação da LGPD trazer à baila o estudo e a pesquisa documental, sobre o instituto e apresentar as ações de prevenção que poderão ser tomadas por essas empresas. A pesquisa que segue foi realizada com base em livros e artigos, não encontrando nenhuma decisão judicial com o mesmo tema como objeto.

Palavras-chave: Lei Geral de Proteção de Dados, Sistema Open Banking, Instituição Financeira, Responsabilidade Civil.

[1] Graduanda do Curso de Direito da Universidade Católica do Salvador. E-mail: karina.carvalho@ucsal.edu.br

[2] Mestre em Estudos Interdisciplinares sobre a Universidade, Pós-Graduado em Processo Civil pela JusPodium, Bacharel em Direito pela Universidade Católica do Salvador – UCSAL, Professor de Direito da Universidade Católica do Salvador. E-mail: carlos.coutinho@pro.ucsal.br.

1 INTRODUÇÃO

A Lei Geral de Proteção de Dados (LGPD) é a lei brasileira para proteção de dados que foi inspirada na GDPR (General Data Protection Regulation), lei de proteção de dados da União Europeia. Desde 2014, com o Marco Civil da internet, o Brasil começou a se deparar com a necessidade de proteção dos dados das pessoas naturais, uma vez que a utilização desses dados de maneira irregular, passou a gerar prejuízo irreversíveis para sociedade,

A publicação da LGPD, aconteceu em 2018 e o Brasil passou a compor um grupo de mais da metade de países do mundo que possuem leis para a proteção dos dados pessoais. A lei é constituída por 64 artigos e seus princípios, que estão definidos no artigo 6º devem observar a boa-fé, Finalidade, Adequação, Necessidade, Livre acesso, Qualidade dos dados, Transparência, Segurança, Prevenção, Não discriminação, Responsabilização e prestação de contas.

Pesquisas realizadas pela Febraban apontam que a cada 10 transações bancárias, 6 ocorrem por meios digitais; evidenciando que a transformação para os meios digitais é uma realidade para as instituições financeira, acentuada pela implementação do sistema Open Banking. O projeto é um novo modelo que viabiliza o compartilhamento de dados entre instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central.Com a implementação desse projeto, o compartilhamento de dados cadastrais dos clientes passa a ocorrer, somente, mediante o expresso consentimento do cliente, que é o proprietário dos dados. A instituição autorizada pelo cliente a acessar esses dados poderá utilizá-los de acordo com a finalidade definida por ele, melhorando a personalização dos produtos e serviços.

No comunicado nº 33.455/2019, o Banco Central estabeleceu os requisitos necessários a implementação do projeto Open Banking Brasil, visando estimular a concorrência do Sistema Financeiro Nacional e do Sistema de Pagamentos Brasileiro, através da promoção de um ambiente de negócio mais inclusivo e competitivo, preservando a segurança do sistema financeiro e a proteção dos consumidores.

O sistema Open Banking Brasil regulamentado pela Resolução Conjunta n° 1 do Conselho Monetário Nacional e do Banco Central, de 4 de maio de 2020 e nessa resolução existe a premissa de que todo o processo deve seguir fundamentado na Lei Geral de Proteção de Dados Brasileira (LGPD).

Diante dos processos judiciais que versam sobre a violação da Lei Geral de Proteção de Dados, constata-se a aplicação de multas e sanções baseadas exclusivamente em seus dispositivos. Valer ressaltar que os processos em andamento indicam que o setor com maior registro de violação aos dados pessoais é o setor bancário, seguidos pelos setores de vendas on-line e telefonia. Portanto, esse indicativo, demonstra a importância do desenvolvimento de iniciativas que proporcionem às instituições financeiras, instrumentos de aderência à Lei Geral de Proteção de Dados.

Como se sabe o direito à privacidade é um direito estabelecido na Constituição de 1988 e busca proteger o indivíduo de invasões de terceiros na sua esfera pessoal. Entretanto, o aumento das transações digitais, vem trazendo uma série de fragilidades na seara de proteção dos dados dos clientes do setor financeiro. Com o sistema Open Banking, os dados pessoais passaram a deter um alto valor de mercado, uma vez que, através deles torna-se possível formar perfis sobre comportamento, consumo, assim como intensificar a concorrência entre instituições financeiras. Portanto, evidencia-se que os interesses do mercado se contrapõem, diversas vezes, ao direito fundamental de privacidade

Nessa perspectiva é que se estabelece a necessidade de uma lei que regule a proteção de dados pessoais garantindo a privacidade dos indivíduos, estabelecendo os direitos e deveres a quem obtêm os dados e os trata. A coleta de informação é uma prática milenar, sendo um dos desafios contemporâneos a preservação desses dados, diante da sua intensa manipulação. Portanto, no atual contexto, à medida que cresce a demanda do mercado pelo armazenamento, tratamento e comunicação dos dados, torna-se mais frágil os sistemas de proteção dessas informações.

A tensão entre o Direito Fundamental à privacidade e os interesses econômicos do setor financeiro tendem a aumentar, na proporção que são intensificadas as trocas de informações dos clientes por meio digital, visando acelerar a concorrências entre as instituições. No atual contexto, as pessoas

estão se tornando objeto de comércio e ficam à mercê de interesses privados dos grandes conglomerados financeiros.

Como apresentado acima, o setor bancário é o responsável pela maior porcentagem de registro de violação aos dados pessoais, sinalizando que o mercado financeiro ainda encontra dificuldades em implementar as diretrizes estabelecidas pela LGPD. Nesse sentido, nos deparamos com a seguinte problemática: qual a responsabilidade civil das instituições financeiras perante o cliente em situações em que os seus dados não sejam coletados, tratados e compartilhados conforme as diretrizes da Lei Geral de Proteção de Dados, em face a implementação do Sistema Open Banking?

Diante de um setor que transaciona diariamente com os dados dos clientes, as instituições financeiras precisam que suas atividades tenham aderência à Lei Geral de Proteção de Dados, visando preservar os dados dos clientes que passaram a ser compartilhados com outra intensidade após a implementação do Sistema Open Banking.

A LGPD busca alcançar a privacidade dos dados pessoais dos usuários a partir do estabelecimento de critérios, regras e práticas para a obtenção, retenção e o processamento de dados. Vale ressaltar, que os objetivos e diretrizes da LGPD são consubstanciados em um arcabouço principiológico, definidos no art. 6º da lei. Esses princípios estabelecem que as empresas precisam desenvolver os procedimentos de coleta, tratamento e transmissão de dados dos seus clientes com transparência, segurança e responsabilização.

A implementação do Sistema Open Banking no Brasil, ao mesmo tempo que incrementou os negócios financeiros, deixou mais vulnerável a proteção de dados dos clientes desse setor. A Autoridade Nacional de Proteção de Dados vem sendo constantemente comunicado acerca das infrações aos procedimentos definidos pela LGPD na seara do mercado financeiro. Portanto, o aumento das transações digitais e o intenso compartilhamento dos dados dos clientes entre as instituições financeiras desafia a implementação da Lei Geral de Proteção de Dados no atual contexto desse setor.

Portanto, o objetivo desse trabalho é analisar a responsabilidade civil das instituições financeiras perante o cliente em situações em que os seus dados não sejam coletados, tratados e transmitidos conforme as diretrizes da Lei Geral de Proteção de Dados, em face a implementação do Sistema Open Banking.

Além de apresentar quais os mecanismos que podem ser pensados visando atenuar ou evitar a responsabilidade civil dessas instituições perante a violação da Lei geral de Proteção de Dados.

2. ASPECTOS GERAIS DA LEI DE PROTEÇÃO DE DADOS (LEI Nº 13.709/2018)

O direito à privacidade é um direito consagrado na Constituição de 1988 e busca proteger o indivíduo de invasões de terceiros na sua esfera pessoal. Portanto, segundo Ferrão (2022, p. 10) a privacidade, no âmbito do direito, pode ser considerada "como o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular".

Os debates sobre privacidade vêm se intensificando ao longo do tempo. Por exemplo, Ferrão (2022, p. 10) considera que o avanço tecnológico, a evolução dos meios de comunicação, o desenvolvimento da internet e o surgimento de redes sociais podem ser considerados marcos na história da privacidade. Uma vez que, os players desses meios registraram um intenso fluxo de informações dos usurários, colocando em risco a privacidade dos seus dados.

Diante da rápida evolução do processamento dos dados, assim como o intenso fluxo de compartilhamento dos dados dos clientes, principalmente entre as instituições financeiras, a preocupação com a privacidade também vem se intensificando com o tempo. Neste cenário de mudanças, leis como a como a GDPR e a LGPD passam a vigorar com o objetivo de alcançar a privacidade dos dados pessoais dos usuários a partir do estabelecimento de critérios, regras e práticas para a obtenção, retenção e o processamento de dados (Ferrão, 2022, p. 10).

É verdade que outras leis já tratavam, de alguma forma, a proteção de dados pessoais, como o Código de Defesa do Consumidor, o Marco Civil da Internet (Lei 12.527/2011), a Lei do Cadastro Positivo (Lei 12.414/2011), dentre outras, mas somente a Lei 13.709/2018 (LGPD) efetivamente regulou o tema.

Enfim, um ponto muito importante ao se abordar a LGPD são os direitos do titular dos dados. Sendo que o mais básico dos direitos previstos no LGPD

trata-se da titularidade dos seus dados pessoais, bem como os direitos fundamentais de liberdade, de intimidade e de privacidade, como visto acima, previstos na Constituição de 1988.

A Lei Geral de Proteção da dados é a lei brasileira para proteção de dados pessoais e foi inspirada na GDPR. Após o marco civil da internet, o Brasil começou a visualizar a proteção dos dados como necessária, uma vez que a coleta, tratamento e compartilhamento de dados em dissonância com a nova legislação pode gerar a responsabilização dos envolvidos nas transações desses dados, convalidando a necessidade de uma lei como a LGPD.

Após a implementação do Regulamento Geral de Proteção de Dados europeu (RGPD ou GDPR na sigla em inglês), a promulgação da Lei Geral de Proteção de Dados brasileira – Lei 13.709/18 representou um avanço, mas seu longo período de *vacation legis* sinaliza a dificuldade de adaptação aos seus ditames. Primeiro, foi editada a Medida Provisória nº 869, de 2018, responsável pelas alterações do texto original. Posteriormente, após diversas audiências públicas com debates a respeito das alterações, foi promulgada a Lei 13.853, de 08 de julho de 2019 que integrou alguns ajustes e manteve alguns dispositivos do primeiro texto.

Segundo Schreiber (2020, p.319) os dados pessoais estão longe de representar “informações sem dono” livremente coletáveis na internet, trata-se de dados que exprimem uma importante projeção da personalidade humana, exigindo proteção da ordem jurídica. No Brasil, a proteção dos dados pessoais encontra seu fundamento na Constituição que tutela a inviolabilidade da intimidade e da vida privada (art.5, CF). Entretanto, doutrina e jurisprudência reconhecem que o direito à privacidade abrange, não apenas à vida intima do indivíduo, mas também a proteção dos seus dados pessoais.

O autor afirma que o direto a proteção de dados pessoais encontrava uma tutela meramente reflexa no direito brasileiro. Sendo abordado apenas por leis esparsas, como o chamado Marco Civil da Internet (Lei 12.965/2014) que apresenta a proteção de dados como seus princípios e o Código de Defesa do Consumidor (Lei 8.078/1990) que estabelece regras específicas sobre bancos de dados e cadastro de consumidores e a lei do Habeas Data (Lei 9.507/1997). Por fim, o autor critica o Código Civil ao apontar que no art. 21º apenas replica inutilmente a disposição constitucional e nada acrescenta sobre o tema. Surge

então a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) assegurando ao titular dos dados um rol de direitos (art. 18), além de disciplinar o tratamento desses dados.

A Lei nº 13.709/2018 dispõe sobre a proteção e o tratamento de dados pessoais, inclusive pelos canais digitais, por pessoa natural ou pessoa jurídica de direito privado ou público. Seu principal objetivo é a proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Com a Lei Geral de Proteção de Dados em vigor, o Brasil passou a compor um grupo de mais da metade de países do mundo que possuem leis para a proteção dos dados pessoais. Segundo dados da organização intergovernamental ligada à ONU, United Nations Conference on Trade and Development (UNCTAD), 66% dos países no mundo possuem alguma legislação relacionada a proteção e privacidade de dados enquanto 19% não possuem nenhuma proposta de lei e 10% estão em processo de elaboração da legislação. A LGPD é constituída por 64 artigos, sendo que no 6º estão consolidados os princípios que norteiam a sua implementação (Ferrão, 2022, p. 12).

Portanto, a Lei Geral de Proteção de Dados coloca o Brasil em situação semelhante aos diversos países que já possuíam regras sobre a proteção de dados e estabelece de forma expressa, a importância da aplicação da boa-fé ao se tratar os dados pessoais, implicando em sanções para as violações através da regulamentação da responsabilidade civil e da reparação dos danos gerados pelos responsáveis pelo tratamento dos dados (Tepedino, Terra, Guedes, 2020, P.290).

A LGPD, em seu artigo 1º, estabelece que o objetivo da lei é proteger “os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”. No artigo 2º, dispõe os seus fundamentos, que são, além da privacidade, a autodeterminação informativa; a inviolabilidade da intimidade, da honra e da imagem; o livre desenvolvimento da personalidade; a dignidade, entre outros (Jarude, Vita, Wandscheer,2020, p. 89).

Conceitos chaves são apresentados no art. 5º, I, ao estabelecer que dado pessoal, nos termos da LGPD, é “informação relacionada a pessoa natural identificada ou identificável” e no art. 5º, II, ao definir que Dado pessoal sensível

é o “dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (Jarude, Vita, Wandscheer,2020, p. 89)..

Ainda sobre conceitos importantes, pode-se esclarecer que tratamento de dados é toda operação realizada com dados pessoais das pessoas física. Vale ressaltar que os responsáveis por esse tratamento são o controlador e operador, chamados de agentes de tratamento. O controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. E o operador é a pessoa natural ou jurídica, de direito público ou privado que realiza o tratamento de dados pessoais em nome do controlador.

Entre os responsáveis pelo cumprimento das normas de proteção de dados temos o encarregado que pode ser chamado de Data Protection Officer (DPO) é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). A ANPD consiste no órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo território nacional, além de penalizar as empresas que não a estiverem cumprindo.

Por fim, a Lei é constituída por 64 artigos e seus princípios, que estão estabelecidos no artigo 6º. Vale ressaltar que esses princípios devem estar em consonância com a boa-fé, dentre eles destacam-se; o princípio da finalidade que estabelece que o tratamento de dados deve ser realizado com uma finalidade específica e legítima, apresentada e consentida pelo cliente, o princípio da adequação que determina que o tratamento dos dados devem ser compatível com a finalidade informada ao cliente, o princípio do livre acesso preconiza que o cliente deve ter permissão de consulta gratuita sobre a forma, a duração do tratamento e a integridade de seus dados pessoais.

Além dos citados acima, o artigo 6º da LGPD apresenta como princípios norteadores; o princípio da transparência que determina que as informações sobre o tratamento de dados devem ser concedidas aos clientes de forma clara, precisa, de fácil acesso e os respectivos agentes de tratamento, observados os

segredos comercial e industrial e por fim, o princípio da responsabilização e prestação de contas que exige a demonstração pelo agente do tratamento que as medidas adotadas foram capazes de cumprir as normas de proteção de dados de uma forma eficaz.

Vale ressaltar que a tramitação legislativa, por mais célere que possa vir a ser, não consegue acompanhar a evolução de determinada matéria, principalmente ao envolver tecnologia, tornando a lei incapaz de prever todas as possibilidades de conflitos da sociedade. Portanto, a aplicação dos princípios torna-se indispensável, por serem responsáveis na orientação da aplicação da lei, possibilitando, por sua vez, atingir eventos futuros, como novas tecnologias e diferentes realidades.

De acordo com a LGPD, em seu art. 7º apresentam-se as bases legais para o tratamento de dados pessoais, estabelecendo as condições que autorizam o tratamento dos dados:

> I-Quando o titular autorizar expressamente o consentimento, sendo importante registrar e manter a sua devida concessão; II. Para a elaboração ou cumprimento de um contrato junto ao titular de dados; III – Para utilização em um possível processo judicial, administrativo ou arbitral; IV -Para o cumprimento de obrigações legais ou regulatórias; V – Para finalidades de proteção ao crédito; VI - Para a realização de estudos por órgãos de pesquisa, garantida sempre que possível a anonimização dos dados pessoais; VII - Para a proteção da integridade física do titular dos dados ou de outra pessoa; VIII -Quando em atendimento de serviços de saúde; IX -Quando necessários com base no legítimo interesse do controlador ou mesmo de um terceiro. (BRASIL, 2018, sem paginação).

Conforme abordado no artigo acima, vale ressaltar que o processamento de dados poderá ser executado pelas instituições de direto privado desde que seja solicitado ao titular do dado o consentimento, que por sua vez, deverá indicar uma finalidade específica. Portanto, não são permitidas autorizações genéricas nem muito menos vícios de consentimento (Ferrão,2022, p.13).

Assim conforme se depreende do art. 8º, § 5º da LGPD, os titulares dos dados têm o direito de revogar o consentimento do tratamento dos seus dados a qualquer momento. Além de autorizar os titulares o acesso a informações, como a finalidade do consentimento, a forma e duração do tratamento, atendendo ao princípio de livre acesso (Ferrão,2022, p.13).

Diante das infrações aos princípios e diretrizes da LGPD, os agentes de tratamento dos dados podem ser punidos com sanções administrativas que

incluem tornar pública a infração após sua apuração e confirmação, suspensão do exercício de tratamento a que refere a infração, multas de até 2% do faturamento da empresa limitado a 50 milhões de reais por infração, entre outros (Ferrão,2022, p.14)

Inclusive, visando inibir essas infrações, os artigos 49º ao 51º a LGPD trazem explicações sobre como devem ser a estruturação dos sistemas de tratamento de dados:

> Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares. (BRASIL, 2018, sem paginação).

Com a necessidade de fiscalização da LGPD foi criada a Autoridade Nacional de Proteção de Dados (ANPD), com a competência estabelecida pelo art. 55º, dentre suas principais funções; a fiscalização da Lei, a comunicação com os controladores dos dados e o estabelecimento de sanções em caso de violação as diretrizes da LGPD (BRASIL, 2018).

Diante do apresentado acima, percebe-se que na nova realidade, o usuário passou a ser o protagonista em relação ao gerenciamento de seus dados. Portanto, o cidadão passou a ser o centro dessa relação através da autodeterminação informativa. Com as normativas GDPR (General Data Protection Regulation) e a LGPD (Lei Geral de Proteção de Dados), o cidadão passou a ter autonomia para acessar, alterar, excluir e escolher compartilhar seus dados com terceiros (Leite, Camargo,2022, p.7).

Em relação à autodeterminação informativa, contata-se que é um conceito importante da lei, seja, por estar relacionada com a hipótese legal do consentimento, seja por estar vinculada ao conceito de privacidade. O novo conceito trata de um direito que consiste ao individuo de ter controle dos seus dados, mesmo estando disponíveis para utilização por terceiros.

Diante do contexto, surge uma nova regulação das relações do sistema financeiro, a implementação do projeto Open Banking. Segundo Leite e Camargo (2022, p.7), quatro fatores foram responsáveis pelo advento dos modelos dos bancos abertos e disrupção regulatória voltada para o compartilhamento de informações: os dados passaram a ser um diferencial para as empresas disruptivas, a criação dos arcabouços legais sobre privacidade, propriedade e

compartilhamento dos dados pessoais, a expansão do mercado das fintechs e por fim, o estímulo das autoridades públicas ao sistema financeiro, tornando-o mais eficiente e inclusivo.

2.1 LGPD E O CÓDIGO DE DEFESA DO CONSUMIDOR

Em relação ao Código de Defesa do Consumidor deve-se salientar que a Constituição Federal atribui ao estado a função de agir na proteção dos consumidores e consequentemente dos seus dados.

Assim, a Constituição ao conceituar e estabelecer as prerrogativas da relação de consumo, acaba identificando a vulnerabilidade do consumidor, assim como, expressamente, no próprio código de defesa do consumidor e, de forma tácita, pela Lei Geral de Proteção de Dados. Segundo (Maimone,2022, sem paginação), essa lei reconhece a assimetria informacional que em conjunto com as regras do novo mercado, acentua a questão da vulnerabilidade.

Em consonância com o apresentado acima, Bioni (2021, P.11) aponta que o dever-direito de informação se traduz na igualdade material entre consumidor e fornecedor em relação a vulnerabilidade informacional, propiciando a parte mais vulnerável (consumidor) autonomia em relação a tomada de decisão. De certa forma essa sistemática da autodeterminação informativa concretiza a tônica de prevenção de danos; bem-informado, dificilmente, o cliente fará um mau negócio e terá prejuízo.

Salienta-se, que o Código de Defesa do Consumidor estabelece uma série de direitos básicos, como: liberdade de escolha (inciso II), a informação adequada e clara (inciso III), proteção contra abuso e práticas abusivas (inciso IV) e a prevenção e reparação de danos (inciso VI). Maimone (2022, sem paginação) afirma que a prevenção de danos é direito básico do consumidor, consequentemente, em situações que necessitam da aplicação do CDC se reconhece a função preventiva da responsabilidade civil abordada na LGPD e no próprio Código de Defesa do Consumidor.

Ainda sobre os dois arcabouços jurídicos, Maimone (2022, sem paginação) aponta que os consumidores se tornam ainda mais vulneráveis quando disponibilizam seus dados para serem utilizados pelas empresas, sendo imprescindível a tutela tanto do CDC, como da LGPD. A defesa do consumidor é um dos fundamentos estabelecido no art. 2º da LGPD, além do art 45º dessa

mesma lei ao estabelecer que responsabilidade civil disposta no CDC deve ser aplicada em casos de violações de dados dos consumidores.

Como apresentado acima, a Lei Geral De Proteção de Dados, está consagrado o princípio da prevenção, no art.6º, inciso VIII ao estabelecer que “adoção de medidas para prevenir a ocorrência de dados em virtude do tratamento de dados pessoais”, em conjunto com o princípio da responsabilização e prestação de conta, positivado no art. 6º, inciso X: “demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive da eficácia dessas medidas” .A autora correlaciona esses artigos da LGPD com o art. 6º, inciso VI do CDC: “ a efetiva prevenção e reparação de danos patrimoniais e morais, individuais, coletivos e difusos”. Portanto, conclui-se que a função preventiva está presente em todo arcabouço jurídico que envolve as relações de consumo e aquelas que são aplicadas a LGPD (Maimone,2022, sem paginação).

3 OPEN BANKING

Diante do novo contexto do Sistema Financeiro nacional, um ambiente com menos barreiras à entrada de novos agentes e, consequentemente, novos modelos de negócios torna-se importante definir e elucidar o conceito Open banking.

Assim, o Banco Central do Brasil, cumprindo sua missão institucional, designou o open banking, como “Sistema Financeiro do Futuro” remodelando o sistema de intermediação financeira, gerando profundas alterações no mercado de crédito, de capitais e de pagamento.

Em março de 2022, o Banco Central publicou a Resolução Conjunta nº 4, alterando as resoluções anteriores e substituindo a denominação Open Banking para Open Finance. Segundo o BACEN, a alteração de nomenclatura foi efetuada com objetivo de expandir a atuação do novo sistema para além dos produtos meramente bancários, passando a englobar também serviços de seguros e previdência, dentre outros produtos financeiros. Apesar da nova denominação, a designação Open Banking permanece sendo utilizada nos

normativos anteriores a março de 2022, por profissionais do Sistema Financeiro, na literatura, por alguns meios jornalísticos de comunicação. Desta forma, optou-se, no escopo deste artigo, em seguir a nomenclatura utilizada pela literatura, preferindo a utilização do termo Open Banking.

O Sistema Open Banking teve seus requisitos fundamentais publicados em abril de 2019, com o comunicado nº 33.455/2019 do Banco Central. Seus princípios são a promoção da concorrência no sistema financeiro, o incentivo à inovação, o aumento da eficiência do Sistema Financeiro, Nacional e do Sistema de Pagamentos Brasileiro e por fim a promoção da cidadania financeira (Ferrão, 2022, p. 17).

De acordo com o Comunicado nº 33.455 do Banco Central, o Open Banking é operacionalizado a partir do compartilhamento de dados, produtos e serviços pelas instituições financeiras e demais instituições autorizadas, de acordo com o consentimento dos clientes, através da integração de plataformas e infraestruturas de sistemas de informação, de forma segura, ágil e conveniente (Jarude, Vita, Wandscheer, 2020, p. 8).

Ainda sobre o processo de regulação do sistema Open Banking, em 5 de maio de 2020 o Banco Central e o Conselho Monetário Nacional publicam o primeiro instrumento normativo para estabelecimento da regulação do Open Banking no Brasil, a Resolução Conjunta nº 1/2020. Nessa Resolução são definidos os participantes obrigatórios do projeto, além de outras instituições financeiras regulamentadas pelo Banco Central que podem participar de forma voluntária (Ferrão, 2022, p. 18).

Conforme o modelo Open Banking, existem três casos de compartilhamento dados e serviços em que a regulamentação vigente estabeleceu a participação obrigatória de alguns agentes (Leite, Camargo,2022, p.7):

> i. No caso de compartilhamento de dados: As instituições financeiras enquadradas na Resolução BCB n. 4.553/2017, com exceção das instituições que integram os conglomerados prudenciais que não prestam os serviços relacionados aos dados transacionais de clientes.
> ii. No caso de compartilhamento de serviço de iniciação de transação de pagamento: as instituições detentoras de conta de depósito à vista ou de poupança ou de pagamento pré-paga, e as instituições iniciadoras de transação de pagamento; e

> iii. No caso de compartilhamento de serviço de encaminhamento de proposta de crédito: as instituições reguladas que tenham firmado contrato de correspondente no país para receber e encaminhar por meio digital, propostas de operação de crédito.

Em sequência, Jarude, Vita, Wandscheer (2020, p. 87) afirmam que as instituições financeiras e as fintechs que não estiverem preparadas para enfrentar a nova geração de transações, serão eliminadas do mercado pelas novas soluções automáticas, em virtude da constante exigência pela redução de custos e de qualidade dos serviços e produtos financeiros. Considera-se fintechs, as empresas ou iniciativas que trazem novas abordagens de negócios em serviços financeiros, de forma escalável, principalmente em razão de tecnologia.

Segundo a Febraban (2019), em 2018 os bancos investiram em tecnologia que aliadas à inteligência artificial, aplicadas para melhorar o relacionamento entre banco e consumidor permitiram a expansão de 2.585% nos atendimentos via chatbots, ferramenta de interação automatizada por robôs que usam linguagem natural e se aperfeiçoam quanto mais são utilizados. Em 2017 foram 3 milhões de interações via chatbots, enquanto em 2018 foram 80,6 milhões. Diante dos dados apresentados pela Febraban, constata-se o crescente investimento dos bancos em tecnologia, visando o acompanhamento das mudanças do Sistema Financeiro Brasileiro.

Portanto, diante desse contexto, deve-se elucidar que o Open Banking é um processo no qual tanto os bancos tradicionais, que já estão se reinventando, quanto às fintechs, desenvolverão produtos e serviços baseados na experiência e no relacionamento com o cliente, por meio de acesso aos dados dos usuários em uma API única. Segundo (Jarude, Vita, Wandscheer, 2020, p. 84) esses compartilhamentos de dados são operacionalizados em virtude de application programming interface (API), ou seja, uma interface de programação de aplicações para integrar os sistemas, permitindo a segurança de dados e facilitando o intercâmbio entre as informações com diferentes linguagens de programação.

Inclusive, a autônoma informacional do consumidor foi um dos elementos cruciais para favorecer a cidadania financeira estabelecida pelo sistema Open Banking sobre a necessidade de obtenção de consentimento. Vale

ressaltar que essa prática foi importada de outras normas, como a Lei Geral de Proteção de Dados Pessoais (LGPD), por exemplo (Leite, Camrago,2022, p.7).

Diante do arcabouço de regras que envolvem os dois institutos, torna-se importante constatar a similaridade no rol de princípios da LGPD e da Resolução Conjunta n° 1 que regulamentou o sistema Open Banking no Brasil. Entretanto, não se pode confundir as regulações. Enquanto as instituições financeiras e instituições autorizadas a funcionar pelo Banco Central do Brasil tratam os dados pessoais de seus clientes de acordo com a LGPD, e observando a regulamentação do Banco Central do Brasil, o compartilhamento de dados e serviços previsto no Open Banking, deve seguir uma regulamentação específica para o consentimento com esta finalidade (Blum,2021, sem paginação).

Ao analisar o tema, percebe-se que a tendência é que o Open Banking ao ser utilizado, conforme seu desenho institucional, tende a ampliar opções aos consumidores e outras soluções inovadoras em um setor marcado por elevada concorrência e que figura entre os mais reclamados nas plataformas geridas pelo governo federal; o setor financeiro (Domingues, Paravela, 2022, p. 84).

Portanto, nesse cenário, o grande desafio enfrentado pelas instituições financeiras será criar os processos adequados para a coleta e gestão do consentimento do cliente, assim como para os processos de transmissão e tratamento desses dados pessoais, em consonância com a Lei Geral de Proteção de Dados (LGPD).

Diante da implementação do Open Banking, surge uma nova prática fundamental no mercado financeiro: a reciprocidade entre as instituições; as participantes passaram a ter o direito de receber dados de seus concorrentes e o dever de compartilhá-los, para isso tornou-se indispensável o consentimento dos clientes. Assim, ocorreu a ampliação da concorrência e favorecimento do maior interessado, o consumidor, que passou a ter em suas mãos a escolha acerca do compartilhamento dos seus dados, por uma via digital e realizado dentro de um ambiente supervisionado pelo Banco Central (Guidolin, Figueiredo,2021, sem paginação).

O fato do open banking ter como premissa o consentimento, uma das bases legais da LGPD (autodeterminação informativa), o cliente poderá a qualquer momento permitir o compartilhamento através de autorização, assim como revogá-lo. Sendo que essa aceitação é específica, ou seja, o cliente está

permitindo apenas que determinados dados sejam partilhados com um banco terceiro, não todos os seus dados, nem para todas as instituições (Guidolin, Figueiredo,2021). Diante dessas questões, surge a necessidade de implementação de uma estrutura de supervisão dessas práticas e um programa de governança.

Ainda segundo os autores, a instituição receptora dessas informações compartilhadas deverá gerenciar o processo de armazenamento desses dados de forma transparente, além de fornecerem para os titulares, um atendimento eficaz e sem burocracia, no momento que resolverem revogar os seus consentimentos ou solicitar esclarecimento a respeito do tratamento e finalidade do uso de suas informações.

4 A PRÁTICA DO SISTEMA BANCÁRIO E O RELACIONAMENTO COM OS DADOS DOS CLIENTES APÓS A IMPLEMENTAÇÃO DO PROJETO OPEN BANKING

De todos os setores da economia, o setor financeiro é, certamente, o que mais utiliza dados pessoais dos clientes. Isso se deve ao fato de que esse tipo de informação é a fonte de execução das atividades do segmento. Portanto, as instituições financeiras precisam cumprir à risca um modelo rígido de governança, com diversas regras restritivas, uma vez que fazem parte de um dos setores mais bem regulamentados.

Cabe mencionar que devido as leis e regulações específicas voltadas para o setor, muitos bancos saíram na frente nos cuidados com a segurança da informação em relação aos dados pessoais tratados. Como exemplo, cumpre menciona a Lei Complementar n.º 105/01 e a Resolução CMN nº 4.658/2018 do BACEN (recentemente atualizada com a Resolução CMN nº 4.893 /2021), essa última que estabeleceu, antes mesmo de a LGPD entrar em vigor, a obrigação de uma política de segurança cibernética e os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

Em dezembro de 2022, os clientes do Sistema bancário passaram a contar com mais um sistema normativo de proteção de dados, em acréscimo à legislação vigente. O normativo SARB 025/21 retrata um novo compromisso do Sistema de Autorregulação Bancária da FEBRABAN (Federação Brasileira dos

Bancos) com a elaboração e implementação de programas de governança em privacidade dos dados dos clientes com requisitos mínimos e boas práticas (Febraban, 2022).

O normativo SARB 025/21 estabelece os princípios e diretrizes que devem ser seguidos pelas instituições financeiras objetivando a proteção dos dados dos clientes, em conformidade com a Lei Geral de Proteção de Dados. Dentre os procedimentos que devem ser adotados, estão previstas, a implementação de um fluxo específico de atendimento aos direitos dos titulares dos dados, estabelecidos na LGPD, estimulando a celeridade e melhorando a qualidade dos serviços financeiros oferecidos aos clientes (Febraban, 2022).

Pela nova norma, como apresentado anteriormente, o conglomerado financeiro nomeia um encarregado de tratamento de dados que será o responsável pela comunicação com a Autoridade Nacional de Proteção de Dados (ANPD), órgão fiscalizador dos dados pessoais que circulam e são coletados e tratados pelas empresas, em conformidade com a LGPD.

Assim como a LGPD determina a nomeação de um "*data protection officer*" (DPO ou encarregado) para coordenar a implantação, fiscalização deste programa. De forma semelhante, a Res. Conj. nº 01/20, que rege o open banking, cria a figura do diretor responsável pelo compartilhamento (DRC). Segundo a LGPD (art. 5º, VII), o DPO é o profissional designado para atuar como ponto de contato entre os agentes de tratamento, os titulares de dados e as autoridades, a Res. Conj. nº 01/20 estabelece (art. 33, §1º) que o DRC é responsável pela elaboração de relatório semestral contendo detalhes sobre o compartilhamento de dados via open banking (Becker et al.2022, sem paginação).

Becker at al (2020, sem paginação) esclarecem que tanto o DPO quanto DRC são funções ligadas à governança corporativa, portanto buscam fiscalizar a relação das instituições com os dados dos clientes, com base em princípios legais como a transparência a prestação de contas e a mitigação do risco de violação de direitos nas atividades de tratamento. Vale ressaltar que a Res. Conj. nº 01/20 determina que a instituição participante do open banking deverá adotar práticas de governança corporativa proporcionais ao risco de sua atividade (art. 37, I), em linha com a Res. CMN nº 2.554/98, a Res. CMN nº 4.553/2017 e a Res. CMN nº 4.557/2017.

Desde a criação do Código de Autorregulação Bancária, temas como atendimento, adequação de produtos ao perfil do cliente, segurança da informação, crédito responsável, proteção aos clientes vulneráveis passaram a ser tratados como principais temáticas sobre relacionamento e proteção ao consumidor.

Apesar de ser um dos setores mais bem regulamentado, o setor financeiro, principalmente após a implementação do projeto Open Banking, enfrenta um desafio que é a forma com que os dados pessoais passaram a ser coletados, tratados e transmitidos entre as instituições financeiras. Enquanto para as empresas do setor é de extrema importância lucrar o máximo com essas informações, sob a ótima da nova regulamentação de dados, a premissa é que essas informações devem ser coletadas tratadas e transmitidas para uma finalidade específica e de acordo com os requisitos estabelecidos na nova legislação.

Como se sabe, os bancos são as instituições mais lucrativas do mercado financeiro, por sua vez, as empresas que mais coletam e tratam dados pessoais. Portanto, um dos grandes desafios enfrentados pelo segmento é compatibilizar a sua cultura voltada para busca incessante por lucratividade e a proteção dos dados dos seus clientes. Dessa forma, adequar a coleta, o tratamento e a manutenção dessas informações a nova lei são os desafios impostos ao setor bancário em uma época de elevado volume de transações digitais (Febraban, 2022).

Segundo Lima et al. (2021 p.103) um dos mais importantes princípios estabelecidos na LGPD é o da transparência, que vai nortear toda aplicação da proteção de dados no setor financeiro. Como visto acima, qualquer transação de coleta, tratamento e transferência de dados só poderá ser concretizada através do consentimento dos clientes. Portanto, qualquer transação envolvendo essas informações devem ser comunicadas com transparência aos seus proprietários, assim como a finalidade e duração do tratamento.

Como se sabe diante da transformação digital da sociedade, os clientes do sistema financeiro passaram a realizar maior parte das transações bancária por canais digitais. Diversos produtos e serviços bancários começaram a ser disponibilizados e comercializados em aplicativos. Assim, como os dados pessoais dos clientes passaram a ser transacionados com outra intensidade, as

operações com que envolvem essas informações foram impactadas, requerendo maiores cuidados.

Entretanto, Ana Frazão (2020, s/p), em importante destaque, afirma que a “violação da privacidade e dos dados pessoais se torna, portanto, um lucrativo negócio que, baseado na extração e na monetização de dados, possibilita a acumulação de um grande poder que se retroalimenta indefinidamente”.

Ainda segundo a autora, nesse fluxo desenfreado, os dados pessoais são compartilhados sem qualquer critério, tampouco controle, visando apenas a lucratividade das operações que utilizam esses dados. Tornando o ambiente empresarial um verdadeiro varejo dos dados pessoais.

Corroborando com o posicionamento apresentado acima, Maimone (2022, sem paginação) afirma que os dados traduzem informações que além de afetarem a privacidade, representam um ativo financeiro, com elevado valor para quem explora o mercado, mas não pelo consumidor, confirmando a assimetria de informação entre esses dois polos da relação consumerista. Dessa maneira, evidencia-se a importância da proteção de dados e da identificação dessas informações como direito da personalidade.

Ainda conforme Maimone (2022, sem paginação) não restam dúvidas que a proteção de dados é reconhecida como direito fundamental e como direito da personalidade, se relacionando com uma série de outros direitos fundamentais cuja violação deve ser prevenida, desencorajada e reprimida.

Diante disso, entende-se que há importante intuito na LGPD de estabelecer a responsabilização das empresas infratoras como consequência às violações à privacidade e à proteção de dados pessoais, estimulando a prevenção de novos danos (Maimone, 2022, sem paginação.). Portanto, a responsabilização das empresas além de ter um caráter punitivo, adentra também na esfera preventiva.

Visto que o mercado está evoluindo para operações dentro do modelo Open Banking, as novas regulamentações trazem novo requisitos para que de um lado seja permitido maior compartilhamento de dados, de forma transparente, e de outro atendendo as exigências de cibersegurança e proteção de dados (Lima et al.,2021, p.103).

Ainda segundo Lima et al. (2021 p. 107), a segurança é umas das principais premissas para gestão de risco no sistema financeiro, portanto um dos

elementos essenciais para estabelecer a relação de confiança entre banco e cliente. Por fim, por mais que os bancos tenham uma estrutura robusta, principalmente, em relação à segurança de informação e façam parte de um dos setores mais bem regulamentados, há uma necessidade de investir em mudança de cultura (Lima et al.,2021 p.113).

Lima et al. (2021, p. 113) elenca uma série de ações que precisam ser instituídas no setor bancário visando essa mudança cultural, como; uma comunicação mais clara, objetiva e transparente com os clientes sobre o tratamento dos dados pessoais, o aperfeiçoamento do sistema de informação de privacidade e de cookies, além da própria gestão de consentimentos nos canais de relacionamento.

Outras frentes necessárias são o treinamento das equipes e o alinhamento com a figura do encarregado de dados, ou também chamado de DPO, uma gestão mais eficaz de riscos relacionados à privacidade e à cibersegurança, assim como uma melhor governança dos dados.

4.1 RESPONSABILIDADE CIVIL

Antes da análise da responsabilidade civil das instituições financeiras perante o tratamento dos dados dos seus clientes após a Lei Geral de Proteção de Dados e a implementação do Projeto Open Banking, torna-se necessário abordar o próprio conceito de responsabilidade civil.

Farias, Netto, Rosenvald (2022, P. 647), conceitua responsabilidade civil, como a reparação de danos injustamente causado, resultantes da violação de um dever geral de cuidado, portanto, é um mecanismo que busca, essencialmente, à recomposição do equilíbrio econômico gerado pelo dano, seja moral, material ou estético.

Durante muito tempo, os juristas se dedicaram a identificar qual teoria se aplicar aos fatos danosos, ou seja, a teoria da responsabilidade objetiva ou a da responsabilidade subjetiva. A teoria subjetiva, clássica, foi construída a partir de quatro pressupostos; ato ilícito, culpa, dano e nexo causal. Portanto, para se ter um dano indenizável, não basta prática de um ato ilícito (contrariedade ao direito e imputabilidade), precisa que seja produzido por ação ou omissão culposa (Farias, Netto, Rosenvald ,2022, p. 658).

Por sua vez, ainda segundo Farias, Netto e Rosenvald (2022, p.690), a teoria objetiva não consagra uma responsabilidade sem culpa, mas uma responsabilidade independentemente da existência de culpa. Ou seja, a culpa poderá existir, mas não é elemento necessário do suporte fático da norma. Portanto, haverá dever de indenizar havendo ou não culpa.

Convém esclarecer que nas duas teorias, o nexo causal tem um papel central na identificação da responsabilidade civil. Segundo Farias, Netto e Rosenvald (2022, p. 690) é filtro de contenção de pretensões reparatórias. Sendo na teoria objetiva, pelo menos em princípio, ainda mais importante, uma vez que não se discute culpa e desloca o centro da discussão da culpabilidade para a causalidade.

Vale ressaltar que não há responsabilidade sem danos, ou seja, o dano é elemento essencial para o mecanismo ressarcitório. O Código Civil brasileiro não conceitua o dano, nem delimita quais seriam as lesões tuteladas pelo ordenamento jurídico, apenas optou por um sistema aberto, em que prevalece uma cláusula geral de reparação de danos.

Ainda sobre dano, Farias, Netto e Rosenvald (2022, p. 662) esclarece que o dano pode violar não só os direitos subjetivos, mas também interesses legítimos. Engloba, não só danos diretos e tangíveis, mas também quebras razoáveis de expectativas e frustações de confiança, entre outras possibilidades. O autor apresenta em sua obra três esferas de danos: patrimonial, moral (extrapatrimonial) e dano estético. Conceitua o dano patrimonial, como “a lesão a um interesse econômico concretamente merecedor de tutela”, o dano moral, como; “uma lesão a interesse existencial concretamente merecedor de tutela”, e por fim define o dano estético, “como a lesão que afeta de modo duradouro o corpo humano, transformando-o negativamente”.

Enfim, após as ponderações sobre os conceitos e teorias da responsabilidade civil, vale ressaltar que atualmente, na maior parte dos ordenamentos jurídicos, competem ao legislador o ao próprio juiz determinar quais atividades se encontram sob a égide da responsabilidade subjetiva ou da objetiva (independentemente de culpa).

Segundo Schreiber (2020, p. 323) não é fácil identificar qual o tipo de responsabilidade civil instituído pela LGPD. Se por um lado, o art. 42º da lei não se refere a culpa, subentende-se um regime de responsabilidade objetiva. Por

outro lado, como o mesmo artigo não apresenta a expressão “independentemente da culpa”, como fizeram o CDC e o Código Civil entende-se a falta da expressão como o indicativo de uma responsabilidade civil subjetiva.

Ainda sobre a divergência, o autor aponta a expressão contida no art.42º que se refere o dano causado “em violação à legislação de proteção de dados pessoais” como uma responsabilidade civil em virtude de uma violação de deveres jurídicos, ou seja, responsabilidade subjetiva.

Schreiber (2020, p.324) ao criticar a técnica legislativa empregada pela LGPD, por não apresentar dispositivos que identifiquem com clareza o tipo de responsabilidade civil, sugere que o intérprete, diante do texto legal sobre a temática, faça sua interpretação conforme os valores constitucionais.

Apesar das falhas das técnicas legislativas empregada na LGPD, serão apresentados alguns posicionamentos doutrinários, visando dirimir as dúvidas sobre o tipo de responsabilidade civil aplicada as instituições financeiras ao violarem a legislação de proteção de dados pessoais.

Como se sabe, a responsabilidade subjetiva é aquela com base na culpa, atualmente conceituada como uma violação a um dever jurídico, portanto segundo Schreiber (2020, p. 325) a responsabilidade aplicada em função de uma violação a um dever jurídico (art. 42) poderia indicar a hipótese da responsabilidade subjetiva.

Outros autores também sustentam a tese que a responsabilidade civil é subjetiva:

Segundo Bione (2022, p. 400) da segunda versão do anteprojeto de lei de proteção de dados, apontou como opção por um regime de reponsabilidade civil subjetiva. Apesar de ter sido amplamente criticada ao longo do segundo processo de consulta pública16 e em audiência pública realizada na Câmara dos Deputados17-18, a responsabilidade civil subjetiva foi a que prevaleceu no Congresso. A redação final da LGPD eliminou os termos anteriormente apresentados – “independentemente de culpa” ou “atividade de risco” – que retiravam a culpa como um dos pressupostos da responsabilidade civil.

Assim, o último estágio da discussão legislativa que são prescritos tais pilares fundantes do regime jurídico da responsabilidade civil da LGPD:

> Em vez de simplesmente espelhar as excludentes do CDC, o legislador optou por eximir a responsabilização dos agentes de tratamento de dados caso comprovem “que, embora tenham realizado o tratamento

> de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados" (art. 43, II). Da mesma forma, quando a LGPD dispõe sobre a responsabilidade civil pela violação à segurança dos dados, há ressalva de que tal responsabilização somente é deflagrada se não foram adotadas as "medidas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação" Trata-se de elementos que afasta a responsabilização do sistema de responsabilidade civil objetiva (Bioni, p.403).

Entretanto, de acordo com Schreiber (2020, p..325) não se pode interpretar os dispositivos das leis de forma isolada, assumindo importância nessa dicotomia, o art. 44º da LGPD:

> 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.
> Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

Assim, não se pode deixar de notar que o artigo apresentado acima, representa uma versão adaptada da noção de defeito de serviço, abordado no art. 14 § 1°, do Código de Defesa do Consumidor. Schreiber (2020, p. 326) esclarece que não seria um absurdo fazer uma analogia com termo "serviço defeituoso" dos dados pessoais, embora a LGPD não apresente esse termo no seu texto. O importante é que a lei geral de proteção de Dados emprega expressão análoga nesta matéria aplicada no CDC, que considera a responsabilidade civil objetiva em relação ao fornecimento de produto e serviço com "defeito".

Em relação a essa temática, Maimone (2023, p.), corrobora com o posicionamento de Schreiber ao defende que a responsabilidade civil estabelecida pela LGPD é objetiva, verificável pela falha no dever de segurança, com a obrigação dos agentes de promover as atividades de tratamento de dados com mecanismos de prevenção, a fim de evitar danos aos titulares a terceiros.

Schreiber (2020, p.327) afirma que não há um posicionamento único em relação a indagação ao tipo de espécie de responsabilidade civil que vigora no âmbito da LGPD.Se por um lado, a lei contempla no parágrafo único no art. 44º

a hipótese de tratamento irregular de dados pessoais em virtude da violação de um dever jurídico, indicativo de responsabilidade subjetiva, por outro lado o fornecimento de segurança inferior a esperada pelo titular dos dados sugere, a responsabilidade objetiva.

Ainda sobre a responsabilidade subjetiva, o parágrafo único do art. 44º, ao se remeter ao art. 46º, abordando a ausência de adoção de medidas protetivas por parte do controlador ou operador, aponta para a responsabilidade civil pelos danos causados (Schreiber, 2020 p.327). Em síntese, percebe-se que a identificação da responsabilidade civil diante de uma realidade fática, torna-se um problema sofisticado e complexo, necessitando da análise da casuística. Portanto, segundo o autor, apesar da redação confusa da legislação, pode-se concluir que convivem os dois regimes distintos; da responsabilidade civil objetiva e da responsabilidade subjetiva.

4.2 RESPONSABILIDADE CIVIL DAS INSTITUIÇÕES FINANCEIRAS NO TRATAMENTO DE DADOS PESSOAIS

Como abordado acima, por diversas vezes, o tratamento de dados se opera no contexto de uma relação de consumo, dessa forma, a art.45º da LGPD consagra que: “As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente”. Apontado por Schreiber (2020, p. 335) o sistema de responsabilidade civil do Código de Defesa do Consumidor, como o mais indicado para proteger os dados pessoais do consumidor.

Aduz o autor (Schreiber,2020 p.335) que não existem drásticas diferenças entre os regimes abordados pelas duas legislações. O regramento do CDC sobre a responsabilidade civil dos fornecedores tem sua fundamentação sobre a questão dos “defeitos” dos produtos e serviços (art. 12 e 14), assim de forma análoga, o conceito de defeito é tratada na segunda parte do caput do art. 44 e seus incisos da LGPD, abordando a valorização da expectativa do titular acerca da segurança do tratamento dos dados.

Diante da referida redação do dispositivo do CDC (art. 2º, § 2º), pode-se afirmar que os direitos dos clientes das instituições financeiras são tutelados por essa legislação. Assim, também, como o art. 3º da mesma legislação prevê o

enquadramento das Instituições Financeiras como fornecedores, uma vez que sua principal atividade é a venda de produtos e a prestação de serviços. E para finalizar, a aplicabilidade do Código nas relações bancárias é ratificada pela Súmula 297 do Supremo Tribunal de Justiça, ao estabelecer que “o Código de defesa do Consumidor é aplicável às Instituições Financeiras”.

Portanto, a abordagem apresentada sobre responsabilidade civil estabelecida no CDC, pode ser aplicado nas relações bancárias, ou seja, danos gerados ao consumidor do setor financeiro por problemas relativos à venda de seus produtos e à prestação dos seus serviços devem ser reparados.

Em sequência, vale ressaltar que o art. 14º do Código de Defesa do Consumidor estabelece a imposição do dever de indenizar para isso exige dano, nexo causal e ocorrência de conduta do agente, independente de culpa, isto é, a responsabilidade civil neste caso é objetiva.

Essa concepção tem sustentação na teoria do risco, um posicionamento jurídico elaborado ao final do Século XIX para justificar a Responsabilidade Civil Objetiva. Para essa teoria, todo dano é imputado ao seu autor e reparado por quem o causou, quando a atividade normalmente desenvolvida pelo responsável do dano implicar, por sua natureza, risco para os direitos de terceiros.

Não se tem como duvidar que o risco é inerente a atividade bancária, principalmente se tratando da segurança de suas transações, como se sabe após a implementação do Open Banking, responsável por intensificar o compartilhamento dos dados entre as instituições, as transações do setor ainda ficaram mais vulneráveis. O sistema de mercado aberto é um importante instrumento de aperfeiçoamento de mercado, principalmente após ser entendido como a expressão da autodeterminação informativa do consumidor, que por sua vez precisa ter a certeza de que seus dados pessoais estarão protegidos em qualquer tipo de transação financeira.

4.3 A ANÁLISE DA RESPONSABILIDADE DAS INSTITUIÇÕES FINANCEIRAS PARTICIPANTES DO OPEN BANKING SOB ORIENTAÇÃO DA LGPD

Segundo Viola, Heringer e Costa (2020, p. 16) um dos pontos controversos relacionados ao sistema Open Banking está em identificar a responsabilidade dos diferentes participantes pela proteção dos dados dos

clientes compartilhados entre as instituições. De um lado, existe a responsabilidade regulatória do controlador original dos dados, do outro a responsabilidade pela obtenção do consentimento do titula, centralizada em quem detém os dados. E ao redor de ambos está a responsabilidade pelos possíveis incidentes.

Apesar da Resolução Conjunta nº 01/2020 determinar que as instituições participantes são responsáveis pela segurança dos dados compartilhados, a norma não individualiza as responsabilidades dos atores (Viola, Heringer, Costa, 2020, p.16). O que se pode afirmar é que do ponto de vista do proprietário dos dados, todos os participantes do sistema serão responsáveis:

> "...pela confiabilidade, pela integridade, pela disponibilidade, pela segurança e pelo sigilo em relação ao compartilhamento de dados e serviços em que esteja envolvida, bem como pelo cumprimento da legislação e da regulamentação em vigor" (art. 31, Resolução Conjunta nº 01/2020

As regras sobre responsabilidade civil estabelecidas pelo Sistema Financeiro Aberto determinam que a instituição que transmite os dados será, a princípio, a responsável pela qualidade das informações transmitidas e, a partir do compartilhamento, essa responsabilidade passará a ser repartida com a instituição receptora, responsável pela conferência da segurança e do sigilo das informações (Viola, Heringer, Costa, 2020, p. 16).

Entretanto, como abordado no capítulo anterior, assim como a responsabilidade civil das instituições financeiras perante os danos dos dados é objetiva, qualquer um dos participantes do Sistema Open Banking também serão responsabilizados pelos prejuízos gerados aos clientes, independente de culpa. Portanto, sempre que houver uma relação de causalidade entre o dano e a participação no sistema, será atraída a responsabilidade objetiva, prevista no Código de Defesa do Consumidor (Viola, Heringer, Costa, 2020, p. 16).

Aduz o autor que individualizar a responsabilidade das instituições participantes do open banking sob a orientação da LGPD não é uma atividade fácil. Conforme o art. 42º a 45º da LGPD, esse processo só se concretiza através da análise de cada situação de compartilhamento de dados, sendo possível delimitar os papéis e responsabilidade de cada participante. Portanto, é importante entender até que ponto a instituição transmissora dos dados atuará

como controladora da operação de tratamento de dados e partir de quando a receptora dos dados assumirá esse papel (Viola, Heringer, Costa, 2020, p. 16).

Em síntese, a criação de um sistema aberto em que diferentes instituições financeiras atuam, compartilhando dados e consequentemente atingindo os múltiplos objetivos do sistema, entre eles, o alcance de um padrão que garanta um nível elevado de autodeterminação informativa, muda drasticamente a configuração do mercado financeiro. Assim não se pode olvidar que o sistema Open Banking, além dos avanços gerados, também aumentou o risco das transações e a responsabilização dos seus participantes.

Em consonância com o exposto, Bione (2022, p.79), sugere como alternativa para atenuar a responsabilidade dos bancos diante a violação das diretrizes da LGPD que se implemente uma estrutura de governança de dados; investindo em capital humano, não apenas tecnológico. Dessa forma, se anteciparão e lucrarão em cima do processo da formação de uma cultura de proteção de dados pessoais ainda a ser formada. Como ocorreu com muitas empresas que se antecederam o marco regulatório estabelecido pelo CDC, agregando valor e reputação aos seus produtos.

CONSIDERAÇÕES FINAIS.

A responsabilidade civil é a único instrumento jurídico que pode ser aplicado quando ocorre uma conduta antijurídica a causar dano a terceiro, sendo que o objetivo do instituto é encontrar o equilíbrio, para restabelecer ou prevenir a situação danosa. Em virtude de sua importância, é um tema em constante debate na doutrina e na jurisprudência.

Conforme o exposto no artigo, conclui-se que a falta de conformidade das Instituições Financeiras com LGPD, por si, já gera responsabilidade civil, ou seja, possibilidade de sanções. As atividades do setor bancário com os dados dos clientes, enquadram a natureza das empresas em um segmento de risco, classificando a responsabilidade dos bancos em objetiva. Portanto, as instituições devem responder pelos danos causados a terceiros, independente de culpa.

Diante do intenso fluxo de compartilhamento de dados entre as instituições, com a implementação do projeto Open Banking, fragilizando a segurança dessas informações, da dificuldade de se individualizar a responsabilidade civil entre os participantes do novo sistema, torna-se importante identificar as ações de prevenção que deverão ser tomadas por essas empresas para evitar futuros processos judiciais.

Deve-se lembrar que o titular dos dados é protegido pelo Código de Defesa do Consumidor, assim como pela LGPD, que colocam o cliente no centro da legislação, portanto todos os procedimentos e boas práticas devem ser implementados pelas instituições participantes do Open Banking, visando resguarda o direito de proteção dos dados desses clientes.

Diante da abordagem de uma temática incipiente, a violação da LGPD em face do projeto Open Banking, não foram encontrados julgados relacionando os dois temas, o que mostra que as constatações apresentadas no trabalho servem como indicativos para evitar futuras judicializações envolvendo as instituições financeiras.

Dentre as soluções pertinentes visando amenizar ou evitar a responsabilização das instituições financeiras perante a violação da Lei Geral de Proteção de Dados, em face a implementação do Projeto Open Banking seria a implementação de uma arquitetura de governança.

O ponto de maior dificuldade deve ser trabalhado como prioridade. Os colaboradores muitas vezes não sabem ao menos o que são dados pessoais, o que se trata o tratamento de dados pessoais, as bases legais que protegem essas transações. Assim como os clientes também não são comunicados com transparência, ética sobre a utilização dos seus dados. Portanto, o que se observa é que a cultura disseminada no ambiente bancário, centrada na busca incessante pelo lucro, torna-se incompatível com um ambiente voltado para o cuidado e zelo com os dados pessoais dos clientes.

A mudança dessa cultura, a implementação de uma boa política de privacidade, a revisão das normas internas da organização e a implementação de uma estrutura de governança são medidas que devem ser adotadas pensando em amenizar ou prevenir a responsabilização das instituições financeiras. Portanto, a preocupação com os direitos dos clientes, a segurança e boas práticas correspondem ao que as empresas necessitam disseminar em

seus ambientes corporativos para enfrentar os desafios oferecidos pelas inovações tecnológicas e mudanças legislativas.

REFERÊNCIAS

ANPD. **Anpd está apurando no caso do vazamento de dados de mais de 220 milhões de pessoas.**2021. Disponível em:<https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-esta-apurando-no-caso-do-vazamento-de-dados-de-mais-de-220-milhoes-de-pessoas>, último acesso em 29 de mar. de 2023.

BECKER, Daniel et al. **DPO e DRC: diálogo entre LGPD e open banking?** 2022. Disponível em <https://www.jota.info/opiniao-e-analise/colunas/regulacao-e-novas-tecnologias/dpo-drc-lgpd-open-banking-29012022>, último acesso em 19 de set. de 2023.

BIONI, Bruno Ricardo. (org.). **Proteção de dados: contexto, narrativas e elementos fundantes.** 2021. Disponível em: < https://observatoriolgpd.com/wp-content/uploads/2021/08/1629122407livro-LGPD-Bruno-Bioni-completo-internet-v2.pdf> Acesso em 20 de set. 2023.

BLUM, Renato Opice, TERADA, Florence M.Dencker**, Open Banking e a Lei Geral de Proteção de Dados.** 2021 Disponível em: < https://febrabantech.febraban.org.br/especialista/renato-opice-blum/open-banking-e-a-lei-geral-de-protecao-de-dados?pesquisa=open%20banking. Acesso em 19 de jul. de 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm. Acesso em: 20 de fev. de 2023.

CALSING, Renata de Assis. **Proteção de dados e autoridade de controle: perspectivas e desafios para o Brasil sob a ótica do direito comparado.** Orientador: Prof. Doutor Pedro Romano Martinez 2019/108p. Tese-Universidade de Lisboa/ Faculdade de Direito,2019. Disponível em: https://repositorio.cgu.gov.br/bitstream/1/66225/3/Tese_Renata_de_Assis_2019.pdf. Acesso em 20 de set de 2023.

DOMINGUES, Juliana Oliveira, PARAVELA, Tatyana Chiari. **Open Banking: a implementação do sistema financeiro aberto no Brasil na perspectiva do consumidor.** 2021. Disponível em: https://revistapgbc.bcb.gov.br/revista/article/view/1133.Acesso em 10 de Jun de 2023.

FEBRABAN. Disponível em: https://portal.febraban.org.br/noticia/3751/pt-br Acesso em: 26 de set de 2023 – **Bancos fortalecem regras para proteger dados pessoais de clientes** - Febraban 2022. Disponível em: https://portal.febraban.org.br/noticia/3751/pt-br/. Acesso em 19 de set. de 2023.

FERRÃO, S.E.R. (2022). **Proposta de uma Taxonomia de Requisitos de Privacidade Baseada na LGPD e ISO/IEC 20100: Aplicação Prática no Open Banking Brasil** orientador: Edna Dias Canedo, 2021. 148 p. Dissertação (Mestrado Profissional) - Universidade de Brasília, Faculdade de Tecnologia, 2021. Disponível em: http: // realp.unb.br> jspui>bitstream> Acesso em: 29 mar. 2023.

GUIDUGLE, Tamiris, FIGUEIREDO, Maurício. **Open banking e LGPD: o desafio dos bancos na proteção de dados.** 2021. Disponível em: https://www.conjur.com.br/2021-jun-26/opiniao-open-banking-lgpd-desafio-bancos-protecao-dados. Acesso em:07 de out. de 2023.

LEITE, Luiza, CAMARGO, Matheus. **Open Banking: inovação aberta no sistema financeiro**. Expressa, 2022.

LIMA, Ana Paula Moraes Canto de... [et al.]; LIMA, Ana Paula Moraes Canto de... [et al.] (coord), **LGPD aplicada.** São Paulo: Atlas, 2021.

MAIMONE, Flávio Henrique Caetano de Paula. **Responsabilidade civil na LGPD**. 1. ed. Indaiatuba: Foco, 2021. E-book. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 21 nov. 2023.

MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (coord.); FALEIROS JÚNIOR, José Luiz Moura (org.). **Responsabilidade civil e novas tecnologias**. 2. ed. Indaiatuba: Foco, 2023. E-book. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 17 nov. 2023.

MENEGAZZI, D. **Um guia para alcançar a conformidade com a LGPD por meio de requisitos de negócio e requisitos de solução**; orientador: Carla Taciana Lima Lourenco Silva Schuenemann, 2021. 111 p. Dissertação (Mestrado em Ciência da Computação) – Universidade Federal de Pernambuco, Recife, Centro de Informática Disponível em: < https://repositorio.ufpe.br/bitstream/123456789/40280/1/DISSERTA%c3%87%c3%83O%20Diego%20Menegazzi.pdf< Acesso em: 20 mar. 2023.

MINISTÉRIO PÚBLICO FEDERAL. **Sistema brasileiro de proteção e acesso a dados pessoais: análise de dispositivos da Lei de Acesso à Informação, da Lei de Identificação Civil, da Lei do Marco Civil da Internet e da Lei Nacional de Proteção de Dados**. Disponível em: https://www.mpf.mp.br/atuacao-tematica/ccr3/documentos-e-publicacoes/roteiros-de-atuacao/sistema-brasileiro-de-protecao-e-acesso-a-dados-pessoais-volume-3, último acesso 29 de março de 2023.

MONTEIRO, Renato Leite. **Desafios para a efetivação do direito à explicação na Lei Geral de Proteção de Dados do Brasil**; orientador Rafael Mafei Rabelo Queiroz, 2021. 391 p. Tese (Doutorado em Direito) - Universidade de São Paulo, Faculdade de Direito, São Paulo, 2021. Disponível em: <https://www.teses.usp.br/teses/disponiveis/2/2139/tde-22072022-120338/pt-br.php >. Acesso em: 20 mar. 2019.

RUARO, Regina Linden. **A tensão entre o direito fundamental à proteção de dados pessoais e o livre mercado.** REPATS - Revista de Estudos e Pesquisas Avançadas do Terceiro Setor, Brasília, v. 4, n. 1, 2017. Disponível em: < https://portalrevistas.ucb.br/index.php/repats/article/view/8212.pdf>, último acesso 29 de mar. de 2023.

TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. **Fundamentos Do Direito Civil – Responsabilidade Civil**. Rio de Janeiro Forense, 2020. v. 4

WANDSCHEER, L. dos S. W.; JARUDE, J. N. D. M.; VITA, J. B. **O Sistema Financeiro Aberto (Open Banking) sob a perspectiva da regulação bancária e da lei geral de proteção de dados.** Revista Brasileira de Filosofia do Direito, [s. l.], v. 6, n. 1,p.78–95,2020.Disponível em: :https://www.indexlaw.org/index.php/filosofiadireito/article/view/6455/pdf Acesso em 11 de jun. de 2023.