OPEN BANKING, PRIVACIDADE E PROTEÇÃO DE DADOS: UMA ANÁLISE À LUZ DA LGPD

Juliana Carolina GNOATTO[1]; **Murilo Henrique GARBIN[2*]**
1. Acadêmica do Curso de Graduação em Direito pelo Centro Universitário de Pato Branco (UNIDEP). E-mail: julianagnoatto@gmail.com. **2.** Mestre em Desenvolvimento Regional pela Universidade Tecnológica Federal do Paraná. Bacharel em Direito pela Universidade Federal do Paraná. Professor do Curso de Bacharelado em Direito do Centro Universitário de Pato Branco (UNIDEP). E-mail: murilo.garbin@unidep.edu.br
Recebido em: 28/10/2022 Aceito em: 16/11/2022

RESUMO: O presente artigo busca tecer uma análise sobre privacidade e proteção de dados no contexto do *open banking* sob a ótica da Lei Geral de Proteção de Dados Pessoais brasileira. Na chamada sociedade da informação, o tráfego de dados pessoais é cada vez mais intenso, o que chama a atenção sobre como se dará sua proteção, inclusive no cenário financeiro, o qual, impulsionado pelas tecnologias digitais, fez surgir o *open banking*, que é um sistema pelo qual as instituições participantes trabalharão com o compartilhamento de dados pessoais de seus clientes. Essa situação, por sua vez, pode trazer uma série de riscos se o tratamento desses dados não ocorrer de forma adequada. Isso posto, com base em revisão bibliográfica e documental, fez-se mister compreender a privacidade e a proteção de dados pessoais na sociedade contemporânea, sobretudo com a inovação trazida pelo sistema financeiro brasileiro à luz da Lei Geral de Proteção de Dados Pessoais, que será esta, como ficou evidente, um importante mecanismo para mitigar os riscos potenciais trazidos pelo *open banking*, sobretudo na proteção de dados pessoais dos usuários.

PALAVRAS-CHAVE: Dados Pessoais. *Open Banking*. Lei Geral de Proteção de Dados Pessoais. Privacidade.

INTRODUÇÃO

Atualmente, vive-se em um cenário em que o uso de tecnologias adquiriu caráter quase que onipresente. Nele, a utilização de dados pessoais pelos meios digitais também aumentou numa escala sem precedentes, inclusive no mercado financeiro, que já possui produtos e serviços totalmente digitais.

O *open banking*, ou sistema financeiro aberto, é um tema atual e de grande relevância, o qual já está alterando e mudará ainda mais o sistema financeiro nacional, visto que permite o compartilhamento de informações entre as instituições participantes, autorizadas pelo Banco Central, por meio de plataformas digitais.

Como o *open banking* trabalha com o compartilhamento de informações de clientes, e sendo eles titulares dos dados de suas contas, a Lei Geral de Proteção de Dados Pessoais (LGPD) assume papel fundamental, sendo imprescindível que as instituições se adequem à referida norma, vez que este compartilhamento não pode ocorrer de forma indiscriminada e deve respeitar a proteção dos dados dos seus titulares.

Com efeito, sabe-se que os dados pessoais no ambiente digital se disseminam rapidamente, atingindo grandes proporções, sobretudo em casos de vazamento. Por terem essa vulnerabilidade, é necessária a utilização de um mecanismo adequado para seus tratamentos

[*]Autor Correspondente

pelas instituições no contexto do sistema financeiro aberto. Ademais, o tráfego de dados nesse novo sistema pode trazer uma série de riscos, comprometendo a própria segurança dos dados pessoais dos clientes.

Por essa razão, é salutar analisar os impactos que a LGPD terá no sistema financeiro aberto, pela ótica da privacidade e da proteção de dados, cuja discussão tem ganhado cada vez mais relevância. Para tanto, vale-se de pesquisa bibliográfica e documental.

Para tanto, fez-se necessário, primeiramente, compreender como será o modelo brasileiro do *open banking* baseado nas diretrizes determinadas pelo Banco Central. Em seguida, foram abordados os desdobramentos históricos que levaram à evolução da tutela da privacidade para a proteção de dados pessoais para, então, ingressar na Lei Geral de Proteção de Dados Pessoais. Cumpre salientar que a pretensão não é de esgotar a análise da norma e nem do tema enfrentado, mas sim abordar alguns aspectos considerados mais relevantes para a presente pesquisa. Por fim, foram analisados os impactos que a Lei Geral de Proteção de Dados Pessoais terá no *open banking.*

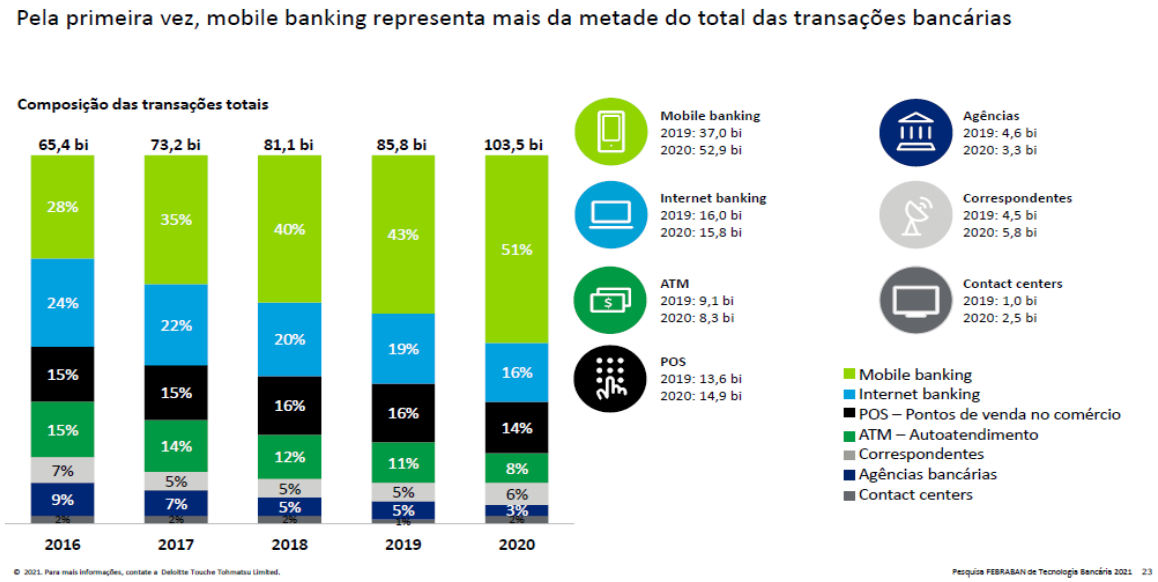
UMA VISÃO DO MODELO BRASILEIRO DE *OPEN BANKING*

O uso de tecnologias que permitem um maior e mais célere fluxo de informações cresceu sem precedentes nas últimas décadas, aumentando a utilização de dados pessoais pelos meios digitais. O mesmo ocorre no mercado financeiro, o qual tem passado por profundas mudanças, sobretudo para atender ao público que exige mais praticidade e está cada vez mais digital (TRINDADE, 2021).

A utilização de canais digitais pelos consumidores tem crescido consideravelmente, especialmente através do *mobile banking*[2], o qual, de acordo com pesquisa da FEBRABAN (2021), representou em 2020 mais da metade das transações bancárias, conforme ilustrado na Figura 1.

[2] *Mobile banking* é um canal digital, acessado por meio de um celular ou *tablet* via aplicativo, que disponibiliza serviços bancários.

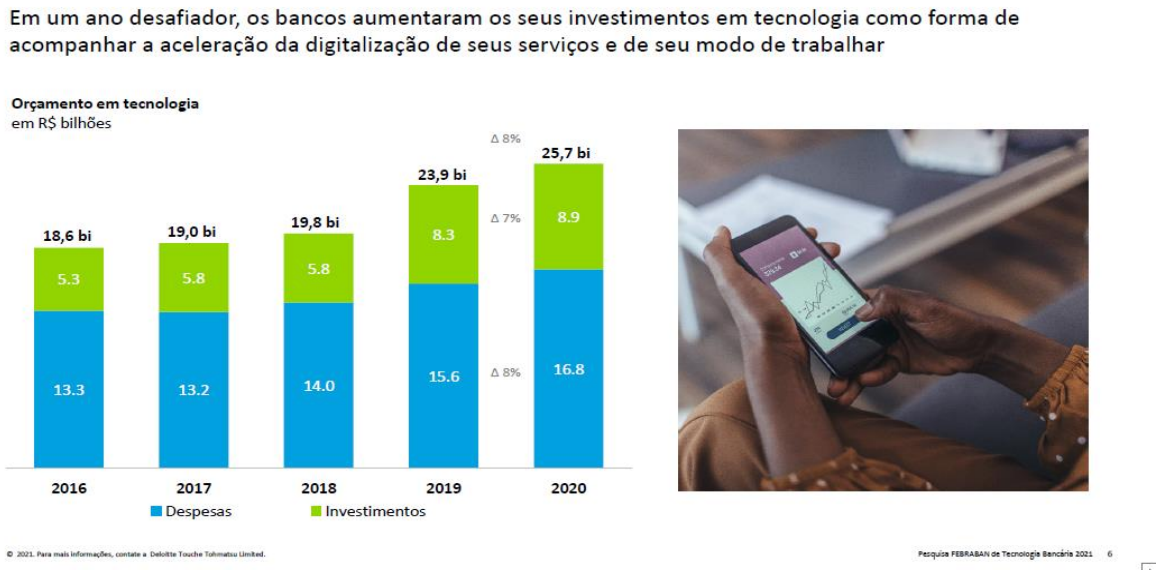
Figura 1 - Transações bancárias realizadas por todos os canais de atendimentos.



Fonte: FEBRABAN (2021).

A adesão dos consumidores pelos canais digitais, mormente pelo *mobile banking*, é reflexo da busca pela comodidade, uma vez que movimentações bancárias podem ser feitas a qualquer momento, independente do lugar, pelo celular (FEBRABAN, 2019). Para acompanhar essa mudança, os bancos estão aumentando a cada ano os investimentos em tecnologias, sendo que, só em 2020, o investimento foi de 25,7 bilhões de reais. A Figura 2 apresenta este aumento de investimentos em tecnologias pelos bancos.

Figura 2 - Investimento em tecnologia, nos anos de 2016 até 2020.



Fonte: FEBRABAN (2021).

Assim, diante desse novo cenário impulsionado pela tecnologia, que promoveu e ainda está promovendo a evolução do mercado financeiro, e o compartilhamento de informações, o *open banking* surge para transformar os serviços financeiros de forma inovadora. Segundo o relatório da FEBRABAN (2021, p. 58) "o *open* banking veio realmente para quebrar paradigmas, inclusive para aprendermos a trabalhar mais juntos e menos no modelo de silos, pensando na jornada do cliente".

O *open banking*, ou sistema financeiro aberto, consoante Comunicado nº 33.455 de abril de 2019 do Banco Central do Brasil[3], consiste num ambiente que permite o "compartilhamento padronizado de dados, produtos e serviços através de abertura e integração de plataformas e infraestruturas" entre instituições autorizadas. Por meio desse sistema, será possível aos clientes o compartilhamento de suas informações entre várias destas instituições.

De acordo com o supracitado Comunicado nº 33.455 e a Circular nº 4.015, as instituições financeiras que irão compor, compulsoriamente, o sistema financeiro aberto são as enquadradas nos segmentos S1, que são aquelas cujo porte é igual ou superior a 10% do Produto Interno Bruto (PIB) ou aquelas que, independente do porte, exerçam atividade internacional relevante; somadas àquelas enquadradas como S2, cujo porte encontra-se entre 1% a 10% do PIB. No que concerne às demais instituições autorizadas a funcionar pelo Banco Central, a opção para participar será facultativa, devendo compartilhar os dados com as outras instituições participantes (BRASIL, 2020; BRASIL, 2019).

O objetivo desse novo sistema, segundo exposto no Comunicado nº 33.455, é trazer eficiência para o mercado de crédito e de pagamento, promovendo a inclusão e a competividade sem abrir mão da segurança dos consumidores e do sistema financeiro (BRASIL, 2019).

A implementação do *Open Banking* no Brasil deu-se em quatro fases, segundo a agenda do BC# (2019), das quais a primeira iniciou no dia primeiro de fevereiro de 2021, a segunda ocorreu no dia 13 de agosto de 2021, a terceira, por sua vez, iniciou no dia 29 de outubro de 2021, e, por fim, a quarta fase deu início no dia 15 de dezembro de 2021 (BCB.GOV, [s.d.]). A Figura 3 esclarece como foi a implementação das quatro fases do *open banking*.

[3] O Comunicado 33.455, de 24 abril de 2019, divulgou os requisitos fundamentais para a implementação do Sistema Financeiro Aberto (*Open Banking*) no Brasil.

Figura 3 - Fases de implementação do open banking.

Fonte: *OPEN BAKING* Brasil [s.d.]

No que tange às informações a serem compartilhadas, o Comunicado nº 33.455, no seu art. 5º, determina o escopo de dados, produtos e serviços que deverão ser compartilhados, os quais devem contemplar:

> I- dados sobre produtos e serviços oferecidos pelas instituições participantes, como características dos produtos, custos financeiros, entre outros; II- dados cadastrais dos clientes, por exemplo, nome, endereço; III- dados transacionais dos clientes, como dados de contas, operações de crédito, produtos e serviços contratados; e IV- serviços de pagamento, que inclui, entre outros, transferências de fundos, pagamentos de produtos e serviços (BRASIL, 2019).

Para que se efetive o compartilhamento das informações dos usuários, é imperioso o consentimento destes, conforme consta no art. 10 da Resolução Conjunta nº 1 de 2020, o qual aduz que, previamente ao início do compartilhamento, deve a instituição receptora dos dados ou iniciadora da transação obter o consentimento do cliente. Para tanto, de acordo com o que preceitua o parágrafo primeiro do mesmo artigo, o consentimento deve ser solicitado de forma clara, objetiva e adequada e deve ser para uma finalidade específica e com prazo de validade compatível para a referida finalidade, sendo a validade limitada em doze meses. Ainda, conforme o parágrafo primeiro do art. 10 da mesma Resolução, devem ser discriminados a instituição transmissora de dados ou detentora de conta, conforme o caso, bem como os dados ou serviços que serão compartilhados, incluindo, também, a identificação do cliente

(BRASIL, 2020).

As etapas para o compartilhamento de cadastro e de transações e serviços são definidas na Resolução Conjunta de 2020, no artigo 8º, e compreendem o consentimento, a autenticação e a confirmação. O compartilhamento de que trata o referido artigo se refere aos dados de clientes e seus representantes e transações de clientes, tais como serviços de iniciação de transação de pagamento (BRASIL, 2020).

O consentimento é a primeira etapa, na qual o cliente autoriza o compartilhamento de seus dados, via aplicativo ou site, para um fim específico. Feita a autorização, segue com a fase de autenticação, em que o cliente será direcionado para outra interface, da instituição de origem, para que ele confirme a finalidade, o prazo do compartilhamento e a instituição que receberá suas informações. Por fim, a fase de confirmação, em que o cliente novamente é redirecionado para a instituição da qual deseja contratar produtos ou serviços, que o notificará de que o compartilhamento foi efetuado (*OPEN BANKING* BRASIL, [s.d.]).

O *open banking* tem o condão de mudar profundamente o cenário do sistema financeiro. Esta mudança permitirá aos usuários, segundo a agenda BC# (2019, p. 9), "transparência e clareza nas informações prestadas; cliente no controle dos seus dados; autenticação semelhante ao acesso direto na instituição e, ainda, simplicidade, segurança e eficiência". Além disso, poderá proporcionar mais competição entre as instituições participantes, dessa forma, podendo ofertar melhores condições em produtos e serviços com menores tarifas (BCB.GOV, [s.d.]).

Os agentes envolvidos no *Open Banking*

A Resolução Conjunta nº 1 de 4 de maio de 2020, nos incisos do seu artigo 2º, define quais são os agentes envolvidos no sistema financeiro aberto (BRASIL, 2020).

O primeiro agente é o cliente, que é qualquer pessoa natural ou jurídica que mantém relacionamentos com instituição financeira autorizada pelo Banco Central, seja através de operações financeiras, prestação de serviços ou transação de pagamentos (BRASIL, 2020).

A instituição receptora de dados, por sua vez, é aquela que, com o intuito de receber dados, solicita o compartilhamento deles junto à instituição transmissora de dados, para que esta os compartilhe. Assim, a instituição transmissora é a que compartilha os dados com a receptora quando solicitado por esta (BRASIL, 2020).

Já a instituição detentora de conta corresponde à instituição em que o cliente possui

conta, seja conta poupança, depósito à vista, ou de pagamento (BRASIL, 2020).

Por seu turno, a instituição iniciadora de transação de pagamento é a instituição que presta serviço, como o próprio nome diz, de iniciação de transação de pagamento, não mantendo consigo os fundos transferidos na prestação de serviço (BRASIL, 2020).

Souto (2020) considera também como um dos agentes o próprio serviço de iniciação de pagamento, o qual consiste no serviço que inicia a instrução de uma transação de pagamento.

Assim, a título de exemplo sobre o funcionamento do *open banking*, a relação entre os agentes envolvidos e as etapas descritas no artigo 8º da Resolução Conjunta, Souto (2020, p. 18) descreve uma operação *on-line*:

> [...] o consumidor (cliente) inicia uma compra (transação) em um *e-commerce* (instituição receptora de dados). O *e-commerce* envia uma requisição de autenticação ao banco do cliente (instituição transmissora de dados). Tendo o banco confirmado a autenticidade do cliente, a instituição iniciadora de transação de pagamento deve obter o consentimento do cliente para compartilhamento dos dados financeiros com o *e-commerce*, conforme o art. 10 da Resolução. Com o consentimento do cliente, o banco autoriza o *e-commerce* a proceder com a conclusão da transação a partir dos dados financeiros dele.

Insta salientar que a referida Resolução impõe que o consentimento, conforme já mencionado, deve preceder o compartilhamento, sendo que, para qualquer alteração nas condições, deve-se obter um novo consentimento, conforme dispõe do artigo 10, § 2º da mesma norma ora citada (BRASIL, 2020).

DO DIREITO À PRIVACIDADE À PROTEÇÃO DE DADOS PESSOAIS

"*Big Data* está vigiando você"; "Os donos dos dados são os donos do futuro". É com estas duas expressões provocativas que Yuval Noah Harari inicia sua narração sobre a liberdade e igualdade, respectivamente, em tempos de algoritmos de vigilância e fluxo de dados[4]. Segundo Harari (2018, p. 107), "[...] no século XXI, os dados vão suplantar tanto a terra quanto a maquinaria como o ativo mais importante, e a política será o esforço por controlar o fluxo de dados".

Com efeito, alguns países já inseriram nos seus ordenamentos jurídicos leis de proteção de dados pessoais com a finalidade dar guarida aos direitos inerentes à pessoa humana que são afetados pelo intenso fluxo de dados, sobretudo a privacidade. A seguir, será

[4] Liberdade e igualdade são dois subtítulos da primeira parte do livro "21 lições para o século 21" escrito por Yuval Noah Harari (2018, p. 69 – 111).

discorrido sobre a evolução do conceito da privacidade para a proteção de dados pessoais e a sedimentação, no Brasil, da Lei Geral de Proteção de Dados Pessoais.

As discussões sobre o direito à privacidade vêm de longa data. Contudo, com a ascensão tecnológica, que passou a permitir o acesso automatizado a informações privadas sobre o indivíduo, veio à tona um novo debate no que tange à sua tutela (MENDES, 2014).

O direito à privacidade é consagrado no ordenamento jurídico pátrio como um direito fundamental, no art. 5º, inciso X, da Constituição Federal de 1988, o qual dispõe: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 1988). Ela pode ser entendida, de acordo com Mendes e Branco (2018), como o direito que o indivíduo tem de não querer deixar ao conhecimento público fatos, informações ou comportamentos de sua vida pessoal. É uma exigência que o indivíduo tem de "encontrar na solidão aquela paz e aquele equilíbrio, continuamente comprometido pelo ritmo da vida moderna" (MENDES; BRANCO, 2018, p. 285, *apud* COSTA JUNIOR, 1995).

Primitivamente, a proteção da privacidade era marcada por um forte individualismo, nutrida, inclusive, por um sentimento egoístico "como o direito a ser deixado só" (RODATÀ, 2008, p. 24) Todavia, as mudanças ocorridas nos modelos de negócio, viabilizadas pela evolução tecnológica, provocaram uma crescente preocupação com a proteção da privacidade e ensejaram novos contornos relativos à sua tutela (DONEDA, 2016; PINHEIRO, 2021).

Essa mudança se deve às diversas formas de organização social ocorridas no decorrer dos anos, aliadas ao desenvolvimento tecnológico, que tornaram possível a capacidade de recolher, processar e utilizar uma imensa quantidade de informações de forma extremamente rápida e pavimentaram o caminho para a atual sociedade, em que a informação é o elemento basilar para o desenvolvimento econômico (BIONI, 2021; DONEDA, 2016).

Bioni (2021) explica que, com essas mudanças, a atividade empresarial foi incrementada pela virtualização da informação, e as empresas passaram a organizar-se em rede, atuando de maneira colaborativa. Isso foi possível em razão da coleta de dados das vendas, utilizados, então, pelas empresas para produção direcionada de bens de acordo com o padrão de consumo.

Com a internet e a evolução das ferramentas tecnológicas, a capacidade de rastrear os dados de navegações dos usuários permitiu que a publicidade fosse direcionada. Os usuários, durante suas navegações na internet, produzem informações sobre suas predileções, tecendo um perfil a ser utilizado para modelar anúncios publicitários de forma personalizada. Esse

mecanismo é conhecido como publicidade direcionada, passando a ser amplamente utilizado pela ciência mercadológica para tornar mais eficiente as publicidades no ambiente virtual (BIONI, 2021).

A publicidade direcionada delineou um caminho utilizado pela ciência mercadológica, transformando esse modelo de mercado com a "monetização dos dados pessoais", e transformou a base de dados relacionados às pessoas em um dos ativos mais estimados, sobretudo com o *Big Data*, o qual possibilita que um volume enorme de dados "seja estruturado e analisado para uma gama indeterminada de finalidades" (BIONI, 2021, p. 23, 34; PINHEIRO, 2021).

A monetização dos dados pessoais reestruturou o mercado econômico, sendo as "informações pessoais a matéria-prima a ser explorada para a geração de riqueza", dessa forma, o comportamento do indivíduo sofre uma observação assídua, com o que é definida como uma economia de vigilância (BIONI, 2021, p. 42).

Como consequência, surge uma nova demanda social: a proteção dos dados pessoais. Estes passaram a ser reconhecidos juridicamente, dada a sua relevância, ultrapassando a mera abordagem do direito à privacidade. Por esta razão, países criaram leis específicas para a proteção de dados pessoais, inclusive no Brasil, que em 2018 promulgou a Lei Geral de Proteção de Dados Pessoais (BIONI, *et al*; PINHEIRO, 2021).

A propósito, é importante enfatizar que o Brasil deu um grande salto no tocante à proteção de dados pessoais. Em 20 de outubro de 2021 foi aprovada a Proposta de Emenda à Constituição (PEC) 17/2019 pelo Senado Federal, que tornou a proteção de dados pessoais, inclusive nos meios digitais, um direito fundamental. Ademais, remeteu à União a competência privativa para legislar sobre a proteção e tratamento de dados pessoais:

> A constitucionalização da proteção de dados como direito fundamental e cláusula pétrea traz avanços significativos para os titulares de dados pessoais e para a garantia dos direitos de privacidade, proteção de dados, e outros direitos, além de deixar ainda mais clara a necessidade de um esforço multissetorial para o fortalecimento de uma cultura de privacidade e proteção de dados no País (GOV.BR, 2021).

A PEC 17/2019 foi encaminhada em 12 de março de 2019 pelo Senador Eduardo Gomes (MDB-TO) com a proposta de incluir a proteção de dados pessoais no rol de direitos e garantias fundamentais, bem como fixar a competência privativa da União para legislar sobre o tema (BIONI; RIELLI; ZANATTA, 2020).

No dia 10 de fevereiro de 2022, foi promulgada pelo Congresso Nacional a Emenda Constitucional 115, que teve origem na PEC 17/2019, incluindo a proteção de dados pessoais

na relação dos direitos e garantias fundamentais, bem como fixou a competência privativa da União "para legislar sobre proteção e tratamento de dados pessoais, conforme a Lei Geral de Proteção de Dados (LGPD)" (GOV.BR, 2022).

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

Como visto, diante do aumento exponencial do fluxo de dados, sobretudo nos meios digitais que facilitam o intercâmbio de informações, há um aumento do risco potencial da utilização dessas informações de forma abusiva, o que motivou a evolução do direito à privacidade, incorporando a proteção de dados pessoais. Surgiu, assim, a necessidade de regulamentar o tratamento desses dados, tendo como pano de fundo a possibilidade de cada indivíduo ter protagonismo sobre as suas informações (MENDES, 2014; RODATÀ, 2008).

Desse modo, para suprir a lacuna no ordenamento jurídico concernente à tutela de dados pessoais, foi criada no Brasil a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), que teve sua gênese a partir do PLC n. 53/2018, sendo promulgada pelo Presidente Michel Temer no dia 14 de agosto de 2018. Segundo Pinheiro (2021, p. 9):

> A Lei n. 13.709/2018 é um novo marco legal brasileiro de grande impacto, tanto para as instituições privadas como para as públicas, por tratar da proteção dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais, por qualquer meio, seja por pessoa natural, seja por pessoa jurídica.

Mendes (2014, p. 32) elucida que referida lei emerge para tutelar a personalidade do indivíduo, o qual, inserido no contexto da sociedade da informação, está submetido aos riscos do tratamento de seus dados pessoais. Logo, disciplinar sobre proteção de dados não traz a função de "proteger os dados *per se*, mas a pessoa que é titular desses dados".

A Lei Geral de Proteção de Dados Pessoais foi orientada pelos marcos regulatórios europeus de proteção de dados, sobre os quais, para engessar as discussões relativas ao tema, foi promulgada a Regulamentação Geral de Proteção de Dados Pessoais Europeu nº 679 (GDPR), aprovada em 27 de abril de 2016, cujo objetivo era a "proteção de dados pessoais e a livre circulação desses dados" por pessoas físicas (BIONI, *et al*; PINHEIRO, 2021, p. 10).

No Brasil, a proteção de dados já era presente, de alguma forma, em outros diplomas infraconstitucionais, quais sejam o Código Civil, o Marco Civil da Internet, o Código de Defesa do Consumidor, a Lei de Acesso à Informação e a Lei do Cadastro Positivo. Assim, a LGPD veio para complementar estas fontes normativas no que tange à proteção de dados pessoais (MENDES; DONEDA, 2018).

Conforme se extrai de seu artigo 1º, a LGPD versa sobre o tratamento de dados pessoais por pessoa natural ou jurídica de direito público ou privado, incluindo os tratamentos pelos meios digitais, cujo objetivo consiste na proteção dos direitos fundamentais de liberdade e privacidade, bem como no desenvolvimento da personalidade da pessoa natural. As normas gerais que constam na lei são de interesse nacional, devendo ser observadas pela União, Estados, Distrito Federal e Municípios (BRASIL, 2018).

Por sua vez, o artigo 2º elenca os fundamentos que regem a disciplina da proteção de dados pessoais, os quais ficam evidentes que estão relacionados com a proteção dos direitos fundamentais inseridos no corpo normativo da Constituição Federal. Os fundamentos presentes na LGPD são: o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre-iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, 2018).

A Lei Geral de Proteção de Dados Pessoais será aplicada, de acordo com o que se depreende de seu artigo 3º, em qualquer operação de tratamento de dados que seja realizada por pessoa natural ou jurídica de direito público ou privado. Ademais, a operação independe do meio, do país da sede ou do país onde estejam localizados os dados, contanto que a operação de tratamento seja realizada no território nacional ou a atividade de tratamento vise à oferta ou ao fornecimento de bens ou serviços ou ao tratamento de dados de indivíduos localizados no território nacional (BRASIL, 2018). Ainda, é necessário que os dados pessoais objeto de tratamento tenham sido coletados no território nacional (BRASIL, 2018).

É importante destacar também que o capítulo VII da LGPD trata da segurança e das boas práticas, as quais devem ser adotadas pelos agentes de tratamento, ou seja, o controlador e o operador - cujas definições serão expostas adiante -, como uma maneira de fomentar a proteção dos dados pessoais de forma eficiente. São medidas contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, incluindo medidas de segurança, medidas técnicas e medidas administrativas (BRASIL, 2018).

Por fim, a Lei Geral de Proteção de Dados Pessoais exibe no seu corpo normativo as sanções administrativas, nos seus artigos 52, 53 e 54, para o caso de infrações cometidas pelos agentes de tratamento de dados, tais como advertência, multa, publicação da infração,

bloqueio dos dados pessoais, entre outras, as quais são aplicáveis pela autoridade nacional, qual seja, a Autoridade Nacional de Proteção de Dados, consoante se extrai do art. 55-A (BRASIL, 2018).

Salienta-se que as sanções da LGPD entraram em vigor somente no dia primeiro de agosto de 2021, quase um ano depois da entrada em vigor da referida lei.

Princípios que regem a Lei Geral de Proteção de Dados Pessoais

A LGPD traz em seu bojo os princípios que regerão as atividades de tratamento de dados. O caput do artigo 6º expressa que para as atividades de tratamento de dados pessoais deve-se observar a boa-fé e os demais princípios que regem a lei (BRASIL, 2018).

O primeiro princípio elencado no artigo 6º da LGPD é o princípio da finalidade, o qual dispõe que o tratamento de dados deve ser para propósitos legítimos, específicos e explícitos (BRASIL, 2018). Deve ser informado ao titular para que finalidade será o tratamento, não havendo a possibilidade de tratamento posterior de forma incompatível com a finalidade. Doneda e Mendes (2018, p. 6) reforçam que deste princípio se depreende que o tratamento de dados pessoais está atrelado à finalidade que "motivou e justificou a sua coleta", sendo, portanto, o tratamento de dados indissociável da função para qual se determina.

Maldonado e Blum (2019, p. 111) esclarecem que os princípios da finalidade, adequação e necessidade estão relacionados entre si e, junto com o princípio da transparência, são essenciais no que concerne à "proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, por meio da tutela dos dados pessoais". Salientam, ainda, que dada a importância do referido princípio, ele expressamente se apresenta em outros três, quais sejam, a adequação, a necessidade e a qualidade dos dados.

O princípio da adequação, vinculado ao da finalidade, conforme dito, define que o tratamento de dados deve ser compatível com as finalidades informadas ao titular, de acordo com o contexto de tratamento (BRASIL, 2018).

O princípio da necessidade, que também se relaciona com os princípios anteriores, limita o tratamento de dados ao mínimo necessário para realizar a finalidade determinada, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados (BRASIL, 2018). Frisa-se aqui que a lei está limitando o

tratamento de dados pessoais, que, para atingir a finalidade a que se pretende, deve ser usado o mínimo de dados necessário, de modo que sejam pertinentes e não excessivos (MALDONADO; BLUM, 2019).

O princípio do livre acesso, por seu turno, garante aos titulares dos dados consulta facilitada e gratuita sobre a forma e duração do tratamento, bem como sobre a integralidade dos seus dados (BRASIL, 2018). Ele fundamenta a autodeterminação informativa e é reforçado pelo artigo 9º da LGPD, o qual aduz que, além do acesso facilitado e gratuito às informações sobre o tratamento, elas deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca da finalidade do tratamento, da forma e da duração, a identificação do controlador e as informações do contato com este, entre outros (MALDONADO; BLUM, 2019).

O princípio da qualidade dos dados impõe a garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento (BRASIL, 2018).

O princípio da transparência dá aos titulares a garantia de que as informações sobre a realização do tratamento e os respectivos agentes de tratamento sejam claras, precisas, e facilmente acessíveis, sendo observados os segredos comercial e industrial (BRASIL, 2018).

A lei traz ainda princípios atinentes à segurança, que impõem a utilização de medidas técnicas e administrativas que sejam aptas a proteger os dados pessoais não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Pelo princípio da prevenção, devem ser adotadas medidas a fim de prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. O princípio da não discriminação estabelece a impossibilidade de realização de tratamento para fins discriminatórios ilícitos ou abusivos. Por último, a responsabilização e a prestação de contas, que consistem na 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 (BRASIL, 2018).

Importante ressaltar, conforme explica Pereira (2020), que o rol do artigo 6º é exemplificativo, não esgotando a matéria. Isso é previsto no artigo 64 da Lei Geral de Proteção de Dados Pessoais, o qual elucida que os direitos e princípios nela expressos não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que o Brasil seja parte.

Conceitos legais

A LGPD traz em seu artigo 5º a definição de dezenove importantes conceitos para sua aplicação, dos quais neste momento alguns merecerão destaque.

A lei define como dado pessoal a informação relacionada à pessoa natural, identificada ou identificável; dado sensível como 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; e dado anonimizado como o dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. O titular é a pessoa natural a quem se referem os dados pessoais que são objetos de tratamento (BRASIL, 2018).

Os agentes de tratamento consistem no controlador e no operador. O controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. O operador, por sua vez, é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; e o encarregado é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) (BRASIL, 2018).

Tratamento, por seu turno, é toda a operação realizada com dados pessoais, como as que se referem à coleta, à produção, à recepção, à transmissão, à distribuição, ao processamento, ao arquivamento, ao armazenamento, à eliminação, à avaliação, ou ao controle da informação, à modificação, à comunicação, à transferência, à difusão ou à extração (BRASIL, 2018).

O consentimento é definido como a manifestação livre, informada e inequívoca, pela qual o titular concorda com o tratamento de seus dados pessoais, para uma finalidade determinada (BRASIL, 2018).

Por fim, a LGPD também traz no rol do artigo 5º as definições de banco de dados, agente de tratamento, anonimização, bloqueio, eliminação, transferência internacional de dados, uso compartilhado da dados, relatório de impacto à proteção de dados pessoais, órgão de pesquisa e autoridade nacional.

Dos requisitos para o tratamento de dados pessoais e dos direitos conferidos aos titulares

Conforme elucidam Mendes e Doneda (2018, p. 472), o tratamento de dados deverá ser realizado a partir de "uma base normativa que o autorize", assim, para que o tratamento seja considerado legítimo, ele deve se enquadrar em pelo menos uma das hipóteses descritas no 7º da LGPD. É uma inovação que não existia ainda no ordenamento jurídico pátrio (DONEDA, 2018). Assim sendo, pelas hipóteses do artigo 7º, somente será realizado o tratamento de dados pessoais (BRASIL, 2018):

> I- mediante o consentimento do titular;
> II - para o cumprimento de obrigação legal ou regulatória, pelo controlador;
> III- pela administração pública, para o tratamento e uso compartilhado de dados à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;
> IV- para a realização de estudos, por órgão de pesquisa, sendo garantido, sempre que possível, a anonimização dos dados pessoais; V- quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI- para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei n. 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> VII- para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII- para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
> IX- para atender aos interesses legítimos do controlador ou de terceiro quando necessário, excetuando-se o caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção do dados pessoais;
> X- ou para proteção do crédito, inclusive quanto ao disposto em legislação pertinente.

Salienta-se que o rol que prescreve os requisitos do tratamento de dados é taxativo, e que, salvo o requisito que exige o consentimento, os demais independem desta exigência. Ademais, como já sublinhado anteriormente, basta o atendimento de uma das bases legais para atingir a legitimidade do tratamento, havendo a possibilidade, mas não necessidade, de sua cumulação (MALDONADO; BLUM, 2019, p. 24).

Ainda, o tratamento de dados pessoais é público e deve atender aos princípios da finalidade, boa-fé e interesse público que justifiquem a sua realização, conforme dispõe o § 3º do artigo 7º. Todavia, não será necessário o consentimento para o tratamento de dados pessoais, conforme consta no § 4º, nas hipóteses em que o próprio titular tornar públicos os seus dados pessoais (BRASIL, 2018). No entanto, mesmo nessas situações, a utilização dos dados não poderá ser utilizada deliberadamente, devendo, pois, serem observados os direitos do titular e os princípios norteadores da LGPD.

No que tange ao consentimento, importante frisar que o artigo 8º da LGPD determina que ele deve ser fornecido por escrito, ou por outro meio que demonstre a manifestação de

vontade do titular, bem como deve referir-se a finalidades determinadas. Além disso, o consentimento pode ser revogado a qualquer tempo, como consta no parágrafo 5º do dispositivo supracitado, mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob o amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação (BRASIL, 2018).

No tocante ao término do tratamento de dados pessoais, previsto no artigo 15, este encerrará nas hipóteses em que for verificado que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; no fim do período de tratamento; com a comunicação do titular, inclusive no exercício do seu direito de revogação do consentimento, resguardado o interesse público; ou com a determinação da autoridade nacional, quando houver violação ao disposto na LGPD (BRASIL, 2018).

Por fim, o artigo 9º da LGPD elenca alguns direitos atribuídos aos titulares dos dados pessoais. O referido dispositivo impõe que o titular tem direito ao acesso facilitado das informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca da finalidade específica do tratamento; forma e duração do tratamento, observados os segredos comercial e industrial; identificação do controlador; informações de contato do controlador; informações acerca do uso compartilhado de dados pelo controlador e a finalidade; responsabilidade dos agentes que realizarão o tratamento; e direitos do titular, com menção explícita aos direitos contidos nos incisos do artigo 18, quais sejam, confirmação, acesso, correção, anonimização, portabilidade, eliminação, informações sobre compartilhamento e sobre a possibilidade de não fornecer consentimento e revogação (BRASIL, 2018).

Consentimento e autodeterminação informativa

A autodeterminação informativa é explicada por Bioni (2021) como o indivíduo, titular dos seus dados, ter o direito de poder controlá-los e poder determinar a sua utilização. Ela é, desse modo, uma "extensão da liberdade do indivíduo" (MALDONADO; BLUM, 2019, p. 24). Por essa razão, a construção legislativa se apoia no consentimento do titular dos dados, em que a autorização do cidadão sobre o fluxo dos seus dados dá a ele o poder de controlá-los.

O consentimento é uma das bases legais do tratamento de dados, conforme consta no artigo 7º, inciso I, da Lei Geral de Proteção de Dados Pessoais, que impõe que somente poderá ser realizado o tratamento de dados pessoais mediante o prévio consentimento do titular. Assim, historicamente, consentimento veio como uma forma de proteção da privacidade e da proteção de dados. Nessa toada, os dados pessoais compõem traços peculiares da personalidade do ser humano, seus valores fundamentais que transcendem sua esfera subjetiva (BIONI, 2021).

Nesse contexto, portanto, tais valores pertencem à personalidade e consistem na forma de como o indivíduo se projeta na sociedade, bem como nos seus direitos consagrados no ordenamento jurídico que são inerentes à pessoa humana (BITTAR, 2015).

Dessa forma, percebe-se que os dados pessoais estão atrelados à personalidade da pessoa como uma projeção direta dela. Consequentemente, o tratamento de dados pessoais pode afetar direitos fundamentais na medida em que influencia no indivíduo enquanto ser social, atingindo sua personalidade (MENDES; DONEDA, 2018). Assim, afirma Bioni (2021, p. 82):

> [...] os dados pessoais não só se caracterizam como um prolongamento da pessoa (subjetividade), mas, também, influenciam essa perspectiva relacional da pessoa (intersubjetividade). A proteção dos dados pessoais é instrumental para que a pessoa possa livremente desenvolver a sua personalidade.

Logo, quando se fala em proteção de dados pessoais, no contexto da LGPD, o dispositivo inicial da lei ampara a proteção dos direitos fundamentais e do desenvolvimento da personalidade.

Nesse cenário, não se pode olvidar que o "objetivo de proteção dos direitos fundamentais e o desenvolvimento da personalidade estão conciliados com os fundamentos da inovação e do desenvolvimento econômico e tecnológico". Com efeito, o que se percebe é a ocorrência de uma colisão entre os "interesses econômicos e as esferas pessoais", na qual o livre desenvolvimento da personalidade resta afetado pelo fluxo de dados pessoais (BIONI, 2021, 109).

Dessa forma, consoante explica o autor ora citado, para atingir uma consonância entre essas duas dimensões, foi proporcionado ao indivíduo o controle sobre os dados. Essa "estratégia vai além do consentimento do titular de dados" e tem como corolário a condição de que o fluxo de informações e o livre desenvolvimento da personalidade devem estar em harmonia, de modo que aquele atenda as expectativas sem prejudicar o desenvolvimento da personalidade (BIONI, 2021, p. 109).

COMPARTILHAMENTO DE DADOS NO ECOSSISTEMA DO *OPEN BANKING* À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Como o *open banking* trabalha com o compartilhamento de informações de clientes através de plataformas digitais, e estes clientes são titulares dos dados de suas contas, a LGPD tem papel fundamental. Por essa razão, é imprescindível que as instituições a ela se adequem, vez que esse compartilhamento não pode ocorrer de forma indiscriminada e deve respeitar o que preceitua a legislação (SOUTO, 2020).

Deve o sistema financeiro aberto, portanto, observar os objetivos e fundamentos da LGPD no tocante à proteção de dados, tais como todos os princípios que constam no artigo 6º que regem o tratamento de dados pessoais, consoante explica Jarude, Vita e Wandscheer (2020), os quais devem ser norteados, ainda, pela boa-fé objetiva.

Devido ao tratamento de dados ter assumido grande relevância, a Resolução Conjunta nº 1 de 2020 do Banco Central inseriu no seu corpo normativo alguns dos princípios presentes na LGPD. Destaca-se o disposto no artigo 4º, o qual prescreve que as instituições que operarão nesse sistema deverão respeitar as leis e as regulamentações em vigor, bem como agir com ética e responsabilidade seguindo os princípios de transparência, segurança e privacidade de dados e de informações sobre serviços compartilhados, qualidade dos dados, tratamento não discriminatório, reciprocidade e interoperabilidade (BRASIL, 2020).

Cumpre ressaltar que, além da importância de o *open banking* estar em harmonia com os princípios, fundamentos e objetivo da Lei Geral de Proteção de Dados Pessoais, também é imperioso o alinhamento com as hipóteses de tratamento de dados pessoais, bem como o atendimento aos direitos dos titulares dos dados que constam na referida norma, enfatizando, ainda, que "a proteção dos dados pessoais dos indivíduos deve ser prioridade no âmbito do *open banking*" (KRASTINS, *et al*; SOUTO, 2020, p. 19).

O sistema financeiro aberto fixa como uma das suas principais bases a autodeterminação informativa, a qual também é um dos pilares da LGDP. À vista disso, o cliente tem autonomia para decidir se quer compartilhar os seus dados ou não com as instituições (KRASTINS, *et al*; SOUTO, 2020).

Por conseguinte, conforme já mencionado, o consentimento, atrelado à autodeterminação informativa, no contexto do *open banking* é condição obrigatória para o compartilhamento das informações. Assim, deve a instituição receptora de dados ou

iniciadora de transação de pagamento obter o consentimento do consumidor. Ressalta-se aqui, conforme elucida Maldonado e Blum (2019, p. 136-137), que "para que o consentimento seja "livre", os titulares devem ter escolha efetiva sobre quais tipos de dados serão tratados em cada operação", ou seja, em caso de coleta de dados para diversas finalidades, deve existir a possibilidade ao titular dos dados de poder escolher para qual finalidade específica ele deseja autorizar o tratamento de dados, "sendo inválido se não houver essa opção".

Ademais, é imperativo que a instituição financeira informe ao cliente para qual finalidade usará os dados por ela solicitados (BRASIL, 2018). Dessa forma, no contexto do *open banking*, Souto (2020) frisa a importância de o consentimento estar alinhado com a Lei Geral de Proteção de Dados Pessoais, devendo ser livre, inequívoco e informado, fornecido por escrito ou por outro meio que demonstre a manifestação da vontade do titular, referindo-se a finalidade determinada.

Insta salientar que o consentimento pode ser revogado a qualquer tempo, conforme o artigo 8º, § 5º da LGPD, por procedimento gratuito e facilitado, sendo manifestado de forma expressa pelo titular, ratificados os tratamentos realizados sob o amparo do consentimento anteriormente manifestado enquanto não houver requerimento da eliminação (BRASIL, 2018).

É importante também que, quando concluído o processo de implementação do *open banking*, faz-se necessário que não haja assimetria de informação entre a instituição e o consumidor (JARUDE; VITA; WANDSCHEER, 2020). Explica Trindade (2021) que a assimetria informacional é quando uma das partes possui mais informações, seja sobre bens, interesses ou condutas de um contratante, podendo assim se aproveitar desta circunstância para incorrer, às custas deste, em vantagens indevidas. Dessa forma, é preciso atenção para verificar se o consentimento do cliente está respeitando os critérios legais, conforme consta no artigo 9º, § 3º da LGPD.

Ainda, salienta Goettenauer (2020, p. 8) a necessidade de estruturação da relação entre o controlador e operador (pela nomenclatura da Resolução Conjunta de 2020 recebem os nomes de instituição transmissora dos dados e instituição detentora da conta; e instituição iniciadora de transação de pagamento, respectivamente) no ambiente do sistema financeiro aberto, para que seja "possível reconhecer esferas de responsabilidade entre cada um dos dois agentes, de maneira a perceber a fragmentação das funções regulatórias".

No que tange aos riscos do *open banking*, frisa-se que, ao mesmo tempo em que o *open banking* cria benefícios tanto para o mercado como para os consumidores, ele traz

consigo potenciais perigos. Para Ribeiro e Bagnoli (2020, p. 221):

> A abertura das informações dos clientes a outras instituições e por tratar de dados financeiros, sensíveis por sua natureza, o modelo também apresenta riscos, bem como dificuldades que devem ser consideradas na avaliação dos reguladores em suas propostas para modelos de implementação.

Dessa forma, o consentimento prévio do cliente, exigido tanto na Resolução Conjunta como na LGPD, é uma das soluções para mitigar os riscos relativos à privacidade dos dados. Da mesma forma, a quebra da assimetria de informação que o *open banking* proporciona também ajuda a diminuir os riscos relacionados à negociação. Para isso, conforme já mencionado, é imperioso verificar se o consentimento do consumidor está dentro dos critérios legais (KRASTINS, *et al*; SOUTO, 2020).

Ainda nesse jaez, é importante que as instituições adotem procedimentos e controles para conter a vulnerabilidade inerente desse novo sistema, sobretudo no desenvolvimento do sistema de informação, conforme exige a LGPD, que consiste na adoção de medidas de segurança, técnicas e administrativas que sejam capazes de proteger os dados pessoais de acessos não autorizados, bem como de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Por fim, conforme salientam Maldonado e Blum (2019, p.122), os agentes de tratamento deverão "durante todo o ciclo de vida de tratamento de dados sob sua responsabilidade, analisar a conformidade legal e implementar os procedimentos de proteção dos dados pessoais de acordo com a sua própria ponderação de riscos". E, em casos de infrações cometidas pelos agentes de tratamento no que tange ao tratamento de dados, ficarão sujeitos às sanções administrativas aplicáveis pela Autoridade Nacional de Proteção de Dados (ANPD).

CONSIDERAÇÕES FINAIS

Considerando todo o exposto, fica evidente a importância que a LGPD exerce sobre o tratamento de dados pessoais, sobretudo no cenário financeiro, no qual, com os avanços da tecnologia, potencializou-se o surgimento de plataformas digitais e a digitalização dos serviços bancários.

O *open banking*, inserido nessa realidade, tem a pretensão de proporcionar menores custos para ofertas de produtos e serviços bancários. Contudo, ele traz riscos que podem comprometer a proteção dos dados pessoais dos consumidores. Assim, a LGPD é um

importante mecanismo para prevenir que o tratamento de dados pessoais realizados pelas instituições financeiras participantes ocorram de forma enviesada e indevida.

Para que esse mecanismo seja de fato efetivo, é mister que as instituições participantes se alinhem à referida norma, de modo que adotem práticas eficientes para a proteção dos dados dos seus clientes.

Outro ponto importante estampado tanto na LGPD como na Resolução Conjunta é o consentimento do cliente, o qual deve ser prévio ao compartilhamento de dados e deve respeitar todos os critérios inseridos na lei, evitando a assimetria informacional e os riscos concernentes à privacidade de dados, tais como aqueles relacionados à negociação. O consentimento é uma ferramenta/instrumento importante que dá ao consumidor o protagonismo sobre os seus dados, permitindo a ele o controle sobre suas informações. Assim, o cliente pode, a qualquer momento, autorizar o compartilhamento dos seus dados, bem como revogá-lo.

Frisa-se que o cliente tem a liberdade de escolher quais dados serão compartilhados em cada operação e com qual instituição, devendo, no caso de uma nova operação, ser solicitado novo consentimento do titular.

Assim, as instituições participantes deverão ter transparência no controle e armazenamento de informações. Ademais, devem atender o usuário de forma prática e eficiente quando forem solicitados esclarecimentos sobre o tratamento de seus dados ou no momento de revogação do consentimento.

Por fim, a LGPD mostra-se como um importante e potencial mecanismo para a proteção de dados pessoais no âmbito do *open banking*, tendo condições de, se aplicada corretamente, mitigar os riscos inerentes a esse sistema.

OPEN BANKING, PRIVACY AND DATA PROTECTION: AN ANALYSIS IN THE LIGHT OF THE LGPD

ABSTRACT: This article seeks to analyze privacy and data protection in the context of open banking from the perspective of the Brazilian General Data Protection Law. In the so-called information society, the traffic of personal data is increasingly intense, which draws attention to how its protection will be given, including in the financial scenario, which, driven by digital technologies, has given rise to open banking, which is a system by which participating institutions will work with the sharing of their customers' personal data. This situation, in turn, can bring a number of risks if the processing of these data does not occur properly. That said, based on bibliographical and documentary review, it was necessary to understand the privacy and protection of personal data in contemporary society, especially with the innovation brought by the Brazilian financial system in the

light of the General Law on Personal Data Protection, which will be, as was evident, an important mechanism to mitigate the potential risks brought by open banking, especially in the protection of users' personal data.

KEYWORDS: Personal Data. Open Banking. General Data Protection Law. Privacy.

REFERÊNCIAS

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento.** 3. ed. Rio de Janeiro: Forense, 2021. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788530994105/epubcfi/6/2[%3Bvnd.vst.idref%3Dcover]!/4/2/2[9ad906f7-0727-4e12-a67f-a93d724944b8]%4050:79. Acesso em: 12 nov. 2021.

BIONI, Bruno Ricardo *et al* (Coords.). **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Ed. Forense, 2021. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788530992200/epubcfi/6/2[%3Bvnd.vst.idref%3Dhtml0]!/4/2/2[d9d9f381-df68-42f7-b3a5-16d907c2469d]%4046:79. Acesso em: 12 nov. 2021.

BIONI, Bruno Ricardo; RIELLI, Mariana; ZANATTA, Rafael. **Comissão Especial Destinada A Proferir Parecer À Proposta De Emenda À Constituição Nº 17-A, de 2019, Do Senado Federal.** Disponível em: https://www.researchgate.net/publication/352799316_Nota_Tecnica_a_PEC_172019_pelo_Data_Privacy_Brasil. Acesso em: 15 jan. 2022.

BITTAR, Carlos Alberto. **Direitos da Personalidade.** 8. ed. São Paulo: Saraiva, 2015. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788502208292/pageid/4. Acesso em: 15 nov. 2021.

BRASIL. Banco Central Do Brasil. **Agenda BC#: *Open Banking*.** Banco Central do Brasil, 2019. Disponível em: https://www.bcb.gov.br/conteudo/home-ptbr/TextosApresentacoes/Open%20Banking%20-%20V07%20-%20Evento%20C4%20-%20S%C3%A3o%20Paulo.pdf. Acesso em: 30 out. 2021.

BRASIL. Banco Central Do Brasil. C**ircular nº 4.015, de 04 de maio de 2020.** Disponível em: https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/51025/Circ_4015_v1_O.pdf. acesso em: 30 de out. 2021.

BRASIL. Banco Central Do Brasil. **Comunicado nº 33.455, de 24 de abril de 2019**. Disponível em: https://www.in.gov.br/en/web/dou/-/comunicado-n%C2%BA-33.455-de-24-de-abril-de-2019-85378506. Acesso em: 30 out. 2021.

BRASIL. **Constituição Federal de 1988**. Promulgada em 5 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 05 set. 2021.

BRASIL. Banco Central Do Brasil. **Open Banking.** Disponível em:

https://www.bcb.gov.br/estabilidadefinanceira/openbanking. Acesso em: 21 ago. 2021.

BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 nov. 2021.

BRASIL. Banco Central Do Brasil. **Resolução Conjunta nº 1, de 04 de maio de 2020**. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-conjunta-n-1-de-4-de-maio-de-2020-255165055. Acesso em: 30 out. 2021.

DONEDA, Danilo. **Da privacidade à proteção de dados.** Editora Renovar, 2016. Disponível em: https://www.academia.edu/23345535/Da_privacidade_%C3%A0_prote%C3%A7%C3%A3o_de_dados_pessoais. Acesso em: 06 set. 2021.

FEDERAÇÃO BRASILEIRA DE BANCOS. **Pesquisa FEBRABAN de Tecnologia Bancária 2021.** Ano-base 2020. Disponível em: https://cmsarquivos.febraban.org.br/Arquivos/documentos/PDF/pesquisa-febraban-relatorio.pdf. Acesso em: 24 out. 2021.

FEDERAÇÃO BRASILEIRA DE BANCOS. **Pesquisa FEBRABAN de Tecnologia Bancária 2019.** Ano-base 2018. Disponível em: https://cmsarquivos.febraban.org.br/Arquivos/documentos/PDF/Pesquisa-FEBRABAN-Tecnologia-Bancaria-2019.pdf. Acesso em: 24 out. 2021.

GOETTENAUER, Carlos. **O Sistema Financeiro Brasileiro, Política de Segurança Cibernética e Proteção de Dados Pessoais: uma Abordagem sob a Ótica da Regulação Policêntrica**. Revista de Direito, Estado e Telecomunicações, Brasília, v. 12, nº 2, p. 172-186. pdf. 2020.

GOVERNO DO BRASIL. **Presidência da República. Autoridade Nacional de Proteção de Dados**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/senado-federal-aprova-proposta-de-emenda-a-constituicao-17-pec-17-2019-que-inclui-a-protecao-de-dados-pessoais-no-rol-de-direitos-e-garantias-fundamentais. Acesso em: 15 out. 2021.

GOVERNO DO BRASIL. **Presidência da República. Autoridade Nacional de Proteção de Dados**. Disponível em: https://www.gov.br/casacivil/pt-br/assuntos/noticias/2022/fevereiro/protecao-de-dados-pessoais-e-incluida-entre-direitos-fundamentais-do-cidadao. Acesso em: 12 mar. 2022.

HARARI, Yuval Noah. **21 Lições para o Século 21.** 1. ed. São Paulo: Companhia das Letras, 2018.

JARUDE, Jamile Nazaré Duarte Monteiro; VITA, Jonathan Barros; WANDSCHEER, Lucelaine dos Santos Weiss. **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, v. 6, n. 1.Jan/Jun. pdf. 2020.

KRASTINS, Alexandra *et al.*; SOUTO, Gabriel (coord). **Relatório LAPIN: Open Banking**

& LGPD: Entraves e Eficiência. Laboratório de Políticas Públicas e Internet (LAPIN), 2020. Disponível em: https://lapin.org.br/2020/11/18/relatorio-open-banking-e-lgpd/. pdf. Acesso em: 18 nov. 2021.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de Dados Comentada.** 2. ed. São Paulo: Thomson Reuters Brasil, pdf, 2019.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional.** 13. ed. São Paulo: Saraiva Educação, 2018. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788553172832/pageid/0. Acesso em: 05 set. 2021.

MENDES, Laura Schertel; DONEDA, Danilo. **Comentários à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil.** Revista de Direito do Consumidor. São Paulo, v. 120, p. 566, 2018.

MENDES, Laura Schertel; DONEDA, Danilo. **Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados.** Revista de Direito do Consumidor. São Paulo, v. 120, 2018.

MENDES, Laura Schertel. **Privacidade, Proteção de Dados e Defesa do Consumidor: Linhas gerais de um novo direito fundamental.** São Paulo: Saraiva, 2014. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788502218987/pageid/0. Acesso em: 15 nov. 2021.

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais.** 3. ed. São Paulo: Ed. Saraiva Jur, 2021. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786555595123/epubcfi/6/2[%3Bvnd.vst.idref%3Dcapa2-0.xhtml]!/4/2/2[e3dc8835-4eb0-4d07-d1fa-157538cd61c6]%4050:79. Acesso em: 12 nov. 2021.

RODATÀ, Stefano. **A vida na sociedade da vigilância: A privacidade hoje.** Rio de Janeiro: Renovar, 2008, pdf.

RIBEIRO, Alexandre Ogêda; 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, pdf, ago./dez., 2020.

SOUTO, Gabriel Araújo. **A cessão de dados financeiros como um Novo Modelo de Negócio através do Open Banking.** Revista PGBC, v. 14, n. 2. Pdf. 2020.

TRINDADE, Manuel Gustavo Neubarth. **Open Banking: Trinômio portabilidade - interoperabilidade - proteção de dados pessoais no âmbito do sistema financeiro.** Revista RJLB, Ano 7, nº 4. pdf. 2021.

VIOLA, Mario; THOMAZELLI, Patrícia. **Portabilidade de Dados, Interoperabilidade e *Open Banking*.** Instituto de Tecnologia & Sociedade do Rio. 2021