Centro Universitário de Brasília - UniCEUB

Faculdade de Ciências Jurídicas e Sociais - FAJS

Curso de Bacharelado em Direito

ANE RODRIGUES DA CRUZ SOUZA

OPEN BANKING: os desafios à proteção de dados pessoais.

BRASÍLIA

2019

ANE RODRIGUES DA CRUZ SOUZA

OPEN BANKING: os desafios à proteção de dados de dados pessoais.

Artigo Científico apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais – FAJSdo Centro Universitário de Brasília (UniCEUB).

Orientador (a): Professor Paulo Rená da Silva Santarém

BRASÍLIA

2019

ANE RODRIGUES DA CRUZ SOUZA

Open Banking: os desafios à proteção de dados pessoais.

Artigo Científico apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais – FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador (a): Professor Paulo Rená da Silva Santarém

BANCA AVALIADORA

_____

Professor (a) Orientador (a)

_____

Professor (a) Avaliador (a)

Open Banking: os desafios à proteção de dados pessoais

Ane Rodrigues da Cruz Souza

Resumo: O presente artigo trata da implementação do *Open Banking* nosistema financeiro brasileiro, no âmbito da proteção dos dados pessoais. Ele busca baseado no exame doutrinário e legislativo, analisar o conceito e o processo regulatório do *Open Banking*, a partir do Comunicado nº 33.455, de 24 de abril de 2019, expedido pelo Banco Central do Brasil, bem como analisar os principais desafios à sua implementação. Ainda, o presente estudo analisa os principais desafios apontados pela doutrina e pelos relatórios técnicos em segurança da informação à proteção dos dados pessoais, no âmbito dos contratos bancários. Diante disso, um dos principais desafios identificados diz respeito à dicotomia entre o desenvolvimento da economia de dados e a necessidade de proteção aos dados pessoais.

Palavras-Chave:*Open Banking.*Sistema Financeiro Aberto.Dados Pessoais. Dados bancários. Sigilo Bancário. Riscos Cibernéticos. Responsabilidade**.**

Este artigo versa sobre a implementação do *Open Banking* no sistema financeiro nacional. Desse modo, busca-se analisar, com base na doutrina e nos dispositivos jurídicos, o processo de abertura dos dados pessoais no âmbito dos contratos bancários.

Sabe-se que a prática de *Open Banking* trará diversos benefícios ao consumidor, como a oferta de serviços personalizados, protagonismo e maior liberdade ao cliente no controle de seus dados. Porém, em contrapartida, há

também diversos desafios para adoção do *Open Banking,* especialmente no âmbito da proteção dos dados pessoais. Assim, o objetivo deste artigo é identificar os desafios apontados pela doutrina jurídica, pelos relatórios técnicos e pesquisas em segurança da informação e proteção de dados.

Para isso, no primeiro tópico, será analisado o conceito de *Open Banking* e modelo regulatório adotado pelo Banco Central do Brasil, tendo em vista a expedição do Comunicado nº 33.455, de 24 de abril de 2019.

No segundo tópico serão identificados os desafios levantados pelos relatórios técnicos e pela doutrina à proteção dos dados pessoais, entre eles a ameaça ao sigilo bancário e os riscos cibernéticos.

Por fim, no último tópico, a partir da leitura de dispositivos jurídico-normativos e de textos doutrinários, serão analisadas as regras cabíveis para a atribuição de responsabilidade no caso de violação à proteção dos dados pessoais no âmbito dos contratos bancários.

A hipótese é que, apesar das inúmeras vantagens do *Open Banking* aos clientes e às instituições financeiras, sua implementação enseja também diversos riscos, principalmente no âmbito da proteção de dados. Assim, as legislações aplicáveis buscam conciliar o interesse do cliente/titular dos dados com os interesses econômicos e financeiros, com base nos princípios e fundamentos que norteiam a Lei Geral de Proteção de Dados.

1. Open Banking

Em pesquisa realizada pela Federação Brasileira de Bancos – FEBRABAN, verificou-se o aumento significativo das realizações de transações bancárias por meio de canais digitais. Hoje, a operações realizadas via *internet banking* ou *mobile banking*, representam um terço das transações bancárias (FEBRABAN, 2019).

Entretanto, esse cenário só foi possível em razão do avanço das tecnologias e do compartilhamento de informações que modificaram a atual forma de desenvolvimento econômico e financeiro e proporcionou desenvolvimento e mudanças nos serviços oferecidos pelos bancos, permitindo a criação de novos modelos de mercado, produtos e serviços.

A prática de *Open Banking* é um exemplo de negócio bancário impulsionado por este novo cenário. Partindo dessas considerações, no tópico a seguir será analisado o conceito de *Open Banking* adotado pelo Banco Central do Brasil, a partir da expedição do Comunicado nº 33.455, de 24 de abril de 2019 e o seu processo de implementação no sistema financeiro nacional.

1.2 Conceito

O Comunicado nº 33.455, de 24 de abril de 2019, expedido pelo Banco Central - BACEN, estabeleceu os requisitos fundamentais para a implementação do Sistema Financeiro Abertono Brasil, conhecido como *Open Banking*. Assim, delimitou as informações que poderão ser compartilhadas entre as instituições financeiras e trouxe uma base sobre como será o funcionamento da plataforma de acesso centralizado dos usuários.

A iniciativa de implementação do *Open Banking* tem como objetivo aumentar a eficiência no mercado de crédito e de pagamentos, mediante a promoção de um cenário de maior inclusão e competitividade, de forma a preservar o equilíbrio do sistema financeiro e, sobretudo, a proteção dos consumidores. Dessa forma, o Banco Central definiu o conceito de *Open Banking* como:

> “compartilhamento de dados, produtos e serviços pelas instituições financeiras e demais instituições autorizadas, a critério de seus clientes, em se tratando de dados a eles relacionados, por meio de abertura e integração de plataformas e infraestruturas de sistemas de informação” (BRASIL, 2019).

De acordo com o Comunicado, os titulares das contas correntes poderão escolher com quem desejam compartilhar informações como dados pessoais, saldo da conta corrente e investimento. Isso se dará por meio de parcerias entres *startups,*

fintechs e empresas de tecnologias, por meio do uso de interfaces de aplicação de programação. (*Application Programming Interface – API*).

Dentre as informações e serviços que poderão ser compartilhados estão produtos e serviços oferecidos pelas instituições participantes (localização de pontos de atendimento, características de produtos, termos e condições contratuais e custos financeiros, entre outros); dados cadastrais dos clientes (nome, número de inscrição no Cadastro de Pessoas Físicas - CPF, filiação, endereço, entre outros); dados transacionais dos clientes (dados relativos a contas de depósito, a operações de crédito, a demais produtos e serviços contratados pelos clientes, entre outros); e serviços de pagamento (inicialização de pagamento, transferências de fundos, pagamentos de produtos e serviços, entre outros), devendo se aplicar às instituições financeiras, instituições de pagamento e demais instituições autorizadas (BRASIL, 2019).

Apesar de que um dos objetivos do Comunicado é concretização da política de abertura de informações bancárias entre as instituições financeiras, o compartilhamento desses dados já era possível no sistema financeiro por meio de resoluções e portarias expedidas pelo Banco Central.

Em 2006, a Resolução nº 3.401, expedida pelo Conselho Monetário Nacional, concedeu autorização para que as instituições financeiras forneçam a terceiros, desde que formalmente autorizados por seus clientes, informações cadastrais:

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

As informações cadastrais que poderiam compartilhadas foram especificadas na Resolução nº 2.835 do Conselho Monetário Nacional, de 30 de maio de 2001.

> a) os dados do cliente, nos termos estabelecidos no art. 1º, inciso I, da Resolução 2.025, de 24 de novembro de 1993, com as alterações introduzidas pelas Resoluções 2.747, de 28 de junho de 2000, e 2.953, de 25 de abril de 2002
>
> b) o saldo médio mensal mantido em conta-corrente;
>
> c) o histórico das operações de empréstimo, de financiamento e de arrendamento mercantil, contendo a data da contratação, o valor transacionado e as datas de vencimentos e dos respectivos pagamentos;
>
> d) o saldo médio mensal das aplicações financeiras e das demais modalidades de investimento mantidas na instituição ou por ela administradas (BRASIL, 2001).

Outrossim, a Lei n° 12.414, de 9 de julho de 2011 (“Lei do Cadastro Positivo”), que disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito, autorizou o compartilhamento de informações cadastrais, bem como as de adimplemento com outros bancos de dados:

> Art. 4º O gestor está autorizado, nas condições estabelecidas nesta Lei, a:
>
> I - abrir cadastro em banco de dados com informações de adimplemento de pessoas naturais e jurídicas;
>
> [...]
>
> III - compartilhar as informações cadastrais e de adimplemento armazenadas com outros bancos de dados (BRASIL, 2011).

Ainda, no mesmo sentido, em 28 de março de 2018, o Banco Central expediu a Resolução nº 4.649 que expõe, indiretamente, um dos principais fundamentos do conceito de *Open Banking:* a possibilidade do cliente, a partir do princípio da autodeterminação informativa, escolher quais serviços financeiros que poderão ser transacionados por meio de sua conta corrente (ou mesmo de pagamento):

> Art. 1º É vedado aos bancos comerciais, aos bancos múltiplos com carteira comercial e às caixas econômicas limitar ou impedir, de qualquer forma, o acesso de instituições de pagamento e de outras

> instituições autorizadas a funcionar pelo Banco Central do Brasil aos seguintes produtos e serviços:
>
> I - débitos autorizados pelo titular de conta de depósitos ou de conta de pagamento mantidas nas instituições mencionadas no caput, inclusive débitos comandados pelo titular da conta por meio de instituições de pagamento ou de outras instituições autorizadas a funcionar pelo Banco Central do Brasil;
>
> II - emissão de boletos de pagamento;
>
> III - transferências entre contas no âmbito da mesma instituição;
>
> IV - Transferência Eletrônica Disponível (TED); e
>
> V - Documento de Crédito (DOC) (BRASIL, 2018)

Apesar da escassez bibliográfica sobre as teorias jurídicas da regulação do sistema financeiro brasileiro, é possível notar que há tempos que o BACEN tem posicionadono sentido de viabilizar a abertura de informações bancárias entre as instituições financeiras. No tópico a seguir, será abordado o processo de implementação e regulamentação do *Open Banking* no país.

1.2 Regulamentação

No diz respeito ao processo de regulação, as diretrizes divulgadas pelo BACEN prevêem que este se dará por duas formas: por meio de edição de atos normativos e por iniciativas de autorregulação.

Os atos normativos poderão ser submetidos à consulta pública, na qual os interessados poderão discutir a definição de escopo, abrangência, responsabilidades, requisitos mínimos para operacionalização do modelo, controles internos, gerenciamento de riscos e condições mínimas para a relação contratual que venha a ser estabelecida entre instituições autorizadas e terceiros não autorizados, além do próprio cronograma de implementação (BRASIL, 2019).

Por outro lado, a autorregulação ficará ao encargo das próprias instituições, as quais serão responsáveis pela padronização das tecnologias e dos procedimentos operacionais, pelos padrões e certificados de segurança e também pela implementação de interfaces, tudo devendo estar em conformidade com a

própria regulamentação. Todavia, o BACEN poderá atuar na coordenação da autorregulação inicial, por meio de revisões e aprovação das decisões, bem como pelo veto, imposição de restrições ou regulação dos aspectos não ajustados. (BRASIL, 2019).

Diante do contexto de inovação tecnológica na oferta de serviços financeiros, os órgãos reguladores do sistema financeiro nacional têm manifestado preferência pela utilização do *Regulatory Sandbox*. Nesse modelo regulatório são elaboradas normas simplificadas e flexíveis, geralmente com um nível de supervisão menor dos reguladores que permitem que novas empresas testem tecnologias diferentes e modelos de negócios inovadores quando elas ainda não têm certeza de sua eficácia (WINTER, 2019).

Uma das vantagens do modelo de *sandbox* para a regulamentação financeira se deve ao fato desse modelo permitir que as empresas validem e testem seus serviços, modelos de negócios, produtos financeiros em um ambiente real de interação com seus consumidores finais, mas ao mesmo tempo de forma controlada e administrado pela autoridade reguladora.

Para Goettenauer(2019), um dos aspectos positivos do modelo de autorregulação é a importância que se dá aos agentes não estatais para a conformação do ambiente regulatório. Dessa forma, a abertura de uma consulta pública prévia antes da apresentação dos atos normativos relativos à regulação das contratações de serviços de tecnologia por instituições financeiras demonstra, de certa forma, um indicativo positivo da abertura do regulador ao diálogo com os regulados e com os demais envolvidos, possibilitando o alcance de maior legitimidade e efetividade dos atos elaborados.

Entretanto, há opiniões divergentes acerca da utilização de mecanismos autorregulatórios. Para Tavares (2010), é necessário observar alguns riscos advindos do processo de autorregulação, como os potenciais conflitos de interesses entre os membros das entidades autorreguladoras e regulados; a utilização pelos auto-reguladores dos poderes a eles conferidos para limitar a competição daqueles

que não são membros, bem como atuação ineficiente dos auto-reguladores, de forma a anular os efeitos da regulação.

Em contrapartida, Bruno Bioni (2019) considera que o modelo de decisão compartilhada permitirá que a autorregulação não atenda interesses apenas de um determinado setor da sociedade ou mesmo do governo, permitindo instaurar um diálogo participativo necessário para tratar de questões complexas próprias da sociedade contemporânea, de maneira a proporcionar o desenvolvimento de um ambiente regulatório mais técnico, possibilitando verticalização e concretização das normas e princípios gerais delineado pela legislação interna, como também das diretrizes delineadas pelos demais autores.

O atual contexto do mercado financeiro demanda mecanismos de regulação mais ágeis e eficazes, sob pena de instaura-se insegurança jurídica, riscos de violação à direitos e simultaneamente redução na inovação de negócios. Dessa forma, é necessário que o sistema jurídico desenvolva instrumentos que garantam estabilidade, segurança jurídica. Dessa forma, conforme afirma Bioni, é necessário que a regulação busque o equilíbrio entre o livre fluxo de informações e a privacidade das pessoas que têm seus dados em trânsito (BIONI, 2019).

Verifica-se que a regulação pode ser considerada como um desafio para a implementação do *Open Banking* no país*.* Por envolver questões importantes sobre compartilhamento de informações das instituições bancária e tratamento de dados pessoais, seu processo de regulação deverá ser pautado padrões de segurança estritamente qualificados, de forma a garantir o avanço das inovações tecnologias, mas que também garanta a proteção dos dados a todos os usuários.

A seguir serão analisadosos desafios levantados pelos relatórios técnicos e pela doutrina à proteção dos dados pessoais, entre eles a ameaça ao sigilo bancário e os riscos cibernéticos, decorrentes da prática de *Open Banking.*

2. Proteção de Dados Pessoais

A proteção de dados pessoais é um fenômeno jurídico recente, cristalizando-se no Brasil com a promulgação da Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).

A LGPD definiu como dado pessoal qualquer “informação relacionada à pessoa natural identificada ou identificável”. Portanto, partindo desse conceito, os dados bancários podem ser enquadrados como dados pessoais, uma vez que a conta bancária possibilita a identificação de informações sobre o titular da conta como, por exemplo, nome, endereço residencial, número de Registro Geral e Cadastro de Pessoa Física e outras informações complementares, como dados financeiros e patrimoniais.

Portanto, considerando que os dados bancários revelam muito sobre a vida privada da pessoa, o sigilo bancário tem a vida privada e a intimidade como bens jurídicos a ser tutelados. A importância da proteção de dados pessoais, no âmbito do direito bancário, pode ser resumida conforme o pensamento do jurista português Diogo Leite Campos:

> Uma parte importante da vida pessoal do cidadão está espelhada na sua conta bancária. A monetarização da economia leva a que, abolida a troca direta, as operações econômicas de cada cidadão sejam efetuadas através de moeda; moeda que circula quase exclusivamente através da conta bancária de cada um. O que cada um veste; o que oferece ao cônjuge e aos filhos; os estudos dos filhos; o volume da sua leitura; as próprias aventuras extraconjugais, tudo é revelável através de uma consulta perspicaz da sua conta bancária. Não constituindo hoje as famílias autarquias econômicas, quase toda a sua vida de relação com os outros é cognoscível através das suas aquisições e vendas de bens e de serviços. Conhecer a conta bancária é conhecer os traços fundamentais da vida privada de cada um; é ter o ponto de partida para conhecer o outro (CAMPOS,1997).

Muito embora a expressão "sigilo bancário" não esteja expressamente prevista na Constituição Federal, a doutrina considera o sigilo bancário, consequentemente os dados bancários, como desdobramento dos direitos à intimidade e privacidade previstos no art. 5º, incisos X da Constituição Brasileira:

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

Nesse sentido, a LGPD estabelece como seu principal objetivo a proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Ainda, tem entre seus fundamentos o respeito à privacidade, a autodeterminação informativa, a inviolabilidade da intimidade e a defesa do consumidor (BRASIL, 2018).

No que diz respeito aos contratos bancários, o direito à proteção ao sigilo bancário é garantido pela Lei Complementar nº 105, de 10 de janeiro de 2001. (“Lei do Sigilo Bancário). No entanto, a Lei do Sigilo Bancário instituiu hipóteses em que o direito/dever de sigilo poderá ser restrito:

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

Porém, de acordo com areferida lei, as instituições financeiras podem compartilhar informações sigilosas, desde que haja o consentimento do cliente. Ainda, nesse mesmo sentido, a Resolução nº 3.401, de 2006, expedida pelo Banco Central do Brasil, estabeleceu em seu art. 3º que:

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

A LGPD determina que o consentimento seja explícito para que os dados sejam recolhidos ou tratados por qualquer organização pública ou privada, salvo disposições contrárias previstas na lei.

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

De igual modo, o Código de Defesa do Consumidor (CDC) outorgou ao consumidor pleno acesso às informações sobre ele lançadas nos bancos de dados, como também fez expressa previsão de proibição de divulgação das informações negativas decorridos cinco anos e impôs também aos cadastros e bancos de dados a baixa de tais informações consumada relativa à cobrança de débitos. Também estabeleceu que para abertura de cadastro, ficha ou registro dos dados pessoais e de consumo deverá haver comunicado escrito ao consumidor, quando não solicitada por ele (EFING, 2000).

Diante um cenário de desenfreada difusão de dados, a preservação do sigilo dos dados bancários é um dos desafios na implementação do *Open Banking*. Para Simões (2016), apesar de ser possível aplicação de legislações esparsas no cotidiano financeiro, a Lei do Sigilo Bancário e a Lei Geral de Proteção de Dados Pessoais não são por si só suficientes para regulamentar a prática do *Open Banking* de maneira determinativa.

2.1 Ameaça ao sigilo bancário e à proteção de dados pessoais

O sigilo bancário pode ser definido como "o dever jurídico que têm as instituições de crédito e as organizações auxiliares e seus empregados de não revelar, salvo justa causa, as informações que venham a obter em virtude da atividade bancária a que se dedicam"(BELINETTI, 1997).

Conforme o pensamento de Hungria (1980), o sigilo bancário é uma condição imprescindível, não só para asegurança do interesse dos clientes do banco como para o próprio êxito da atividade bancária, Entretanto, no conhecimento da vida financeira de seus clientes, o agente bancário está adstrito a silêncio em torno de quaisquer fatos que, se revelados ou comunicados a terceiros, acarretariam àqueles efetivo ou possível dano.

Contudo, o sigilo bancário e, por consequência a prática de *Open Banking*, foi afetada com a edição da Lei n° 12.414, de 9 de julho de 2011 (“Lei do Cadastro Positivo”), que disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito.

Inicialmente, o texto da Lei do Cadastro Positivo previa a utilização do sistema *opt-in,* no qual haveria necessidade de prévio consentimento para que o titular dos dados pessoais de crédito autorizasse à abertura de seu cadastro e dados sejam coletados, armazenados e tratados (BIONI, 2019).

Entretanto, com a aprovação da Lei Complementar nº 166, de 4 de abril de 2019, a adesão ao cadastramento ao banco de dados do sistema do Cadastro Positivo passa a ser realizado pelo sistema *opt-out*, ou seja, de forma automática e prescinde qualquer tipo de consentimento prévio. O gestor responsável pelo banco de dados deverá, entretanto, informar o titular em até 30 dias após a abertura, e notificar quais são os canais de comunicação para que o indivíduo manifeste posteriormente sua discordância e faça solicitação de cancelamento do cadastro (BIONI, 2019).

A alteração da Lei de Cadastro Positivo contraria os dispositivos do Código de Defesa do Consumidor, da Lei de Sigilo Bancário e, principalmente, a Lei Geral de Proteção de Dados, em um dos seus aspectos mais importantes, que é autodeterminação informativa do cidadão, pois permite a abertura de cadastro e compartilhar informações cadastrais com outros bancos de dados:

> "Art. 4º O gestor está autorizado, nas condições estabelecidas nesta Lei, a:
>
> I - abrir cadastro em banco de dados com informações de adimplemento de pessoas naturais e jurídicas;
>
> II - fazer anotações no cadastro de que trata o inciso I do caput deste artigo;
>
> III - compartilhar as informações cadastrais e de adimplemento armazenadas com outros bancos de dados; e
>
> IV - disponibilizar a consulentes:
>
> a) a nota ou pontuação de crédito elaborada com base nas informações de adimplemento armazenadas; e
>
> b) o histórico de crédito, mediante prévia autorização específica do cadastrado. (BRASIL, 2018)

O *Open Banking*, ao reger-se pela LGPD e pelo CDC, parte do princípio que para que haja o compartilhamento das informações cadastrais contidas nos bancos de dados, deve haver o consentimento escrito do titular dos dados. Nota-se que para a LGPD, consentimento é manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (BRASIL, 2018).

Logo, ao permitir o compartilhamento as informações cadastrais e de adimplemento armazenadas com outros bancos de dados sem o consentimento do titular de dados, a Lei Complementar nº 166/2019 poderá trazer inseguranças jurídicas quanto à exigência de consentimento também para prática de *Open Banking.*

Ainda, de acordo com Bruno Bioni, a adoção de uma sistemática *opt-out*, que transfere a capacidade do cidadão de controlar seus dados pessoais para após que eles já estarem sendo tratados, acaba-se por marginalizar a sua carga participativa, artificializando a autodeterminação informacional e reduzir a carga participativa do cidadão quanto ao fluxo de suas informações pessoais. (BIONI, 2019)

Segundo Danilo Doneda, o direito à autodeterminação informativa tem status de direito fundamental por tratar-se de direito de personalidade, o que garante, de per si, ao indivíduo, o poder de controlar as suas próprias informações, sendo uma afirmação do personalíssimo no âmbito das interações entre indivíduo e sociedade. (DONEDA, 2006)

Importante ressaltar que, de acordo com Valente (2006), o bem jurídico tutelado pela Lei do Sigilo Bancário não são os dados propriamente dito, mas sim a troca de informações sobre tais dados. Logo, a comunicação sobre os dados bancários não pode ser violada por terceiros.

2.2 Riscos cibernéticos

A proteção de dados pessoais é orientada por cinco princípios: o princípio da publicidade, princípio da exatidão, princípio da finalidade, princípio do livre acesso e, por fim, pelo princípio da segurança física e lógica. Considerando o princípio da segurança física e lógica, os dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado (DONEDA, 2006).

Em pesquisa realizada pela PCW (2018), demonstrou-se que os riscos cibernéticos estão como a principal ameaça aos serviços financeiros digitais. E, com a diversificação de canais, disseminação de serviços em nuvem e com o avanço do *Open Banking,* a tendência é que a questão da segurança cibernética torne-se ainda mais desafiadora.

A maioria das falhas em segurança da informação associadas à tecnologia está relacionada ao vazamento, perda e mau uso da informação (figura 2), seja pela manipulação incorreta da informação ou pela falta de uma política de segurança clara e bem definida (PTI, 2016).

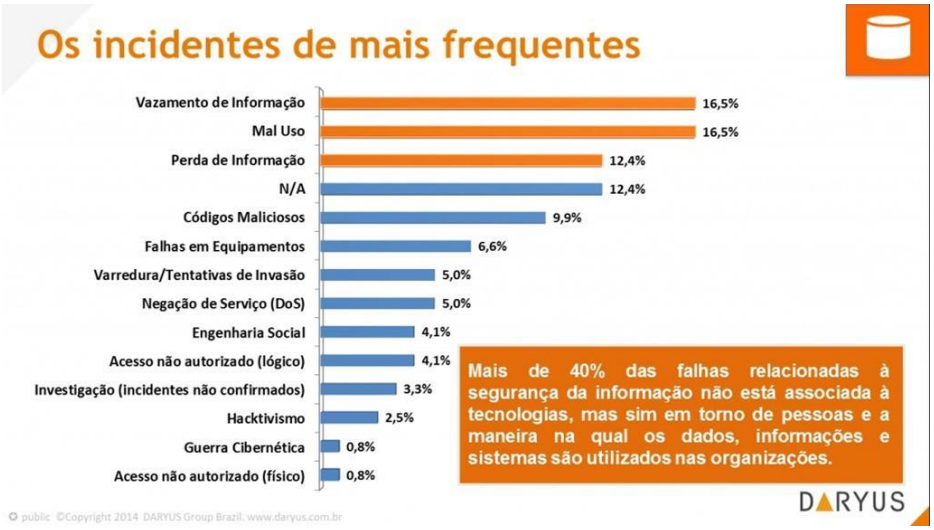

Figura 2– Incidentes mais frequentes

Fonte: PTI, 2016.

Nesse sentido, diante desse cenário de inclusão de novas tecnologias no setor financeiro e a crescente interação entre os sistemas tecnológicos das instituições financeiras e de outros parceiros comerciais, o BACEN publicou o Edital de Consulta Pública nº 57 de19 de setembro de 2017.

A consulta pública resultou na elaboração da Resolução nº 4.658 de 26 de abril de 2018, que dispõe sobre apolítica de segurança cibernética e os serviços de processamento e armazenamento de dados em nuvem e de computação em nuvem a serem observados por instituições financeiras e estabeleceu requisitos mínimos que deverão ser contemplados na política de segurança cibernética de uma instituição financeira:

> Art. 3º A política de segurança cibernética deve contemplar, no mínimo:
>
> [...]

> III - os controles específicos, incluindo os voltados para a rastreabilidade dainformação, que busquem garantir a segurança das informações sensíveis;
>
> V - as diretrizes para:
>
> c) a classificação dos dados e das informações quanto à relevância; e
> VI - os mecanismos para disseminação da cultura de segurança cibernética nainstituição, incluindo:
>
> [...]
>
> b) a prestação de informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros (BRASIL, 2018).

Ainda, no que diz respeito aos procedimentos e os controles adotados para reduzir a vulnerabilidade da instituição financeira aos incidentes e atender aos demais objetivos de segurança cibernética, a referida resolução determinou adoção de procedimentos mínimos de segurança da informação:

> § 2º Os procedimentos e os controles de que trata o inciso II do caput devem abranger, no mínimo, a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações (BRASIL, 2018)

A inserção tecnológica no ambiente bancário permitiu o desenvolvimento de uma linguagem uniforme para que o uso, a transformação e a transmissão de informações sejam amplos e difundidos de maneira global e universal. Em contrapartida, este cenário acabou tornando-se vulnerável atraindo um grande número de indivíduos mal-intencionados, que se aproveitando da ausência de informação de alguns clientes para perpetrar fraudes eletrônicas

As relações jurídicas existentes entre os clientes e as instituições bancárias e financeiras, em decorrência da própria atividade desenvolvida, impõem necessidade de absoluta confiança. Dessa forma as instituições deverão

desenvolver modelos de autenticação seguros de forma a possibilitar a identificação de quem enviou determinado conjunto de dados, a finalidade e o destino, a fim de evitar a violação de dados e acesso não autorizado.

3. Responsabilidade por danos

No ordenamento jurídico brasileiro há estruturas relacionadas às atividades financeiras exercidas pelo Estado, como também há atividades bancárias exercidas pelas instituições financeiras e bancárias. Assim sendo, essas atividades são reguladas tanto por normas do direito público e por disposições normativas de direito privado. Diante dessa característica, a aferição da responsabilidade civil nos contratos bancários é um tema complexo, devendo deve ser analisada sob perspectiva do direito civil-constitucional (ESTEVES, 2011).

As fontes normativas sobre a responsabilidade civil nos contratos bancários decorrem do Código Civil e o Código de Defesa do Consumidor, além das normas de direito bancário e resoluções do Banco Central.

O contrato bancário, na qualidade de negócio jurídico, poderá ensejar a responsabilidade civil quando configurada a ilicitude do negócio ou se o ato originado dele caracterizar um ato ilícito. Assim, nos termos do art. 927, parágrafo único, do Código Civil, a responsabilidade será pautada no plano subjetivo ante o dever de reparar o dano. Contudo, a responsabilidade poderá ser objetiva, em virtude da aplicação da Lei nº 7102/1983, que atribui aos bancos o dever de segurança ao público em geral (ESTEVES, 2011).

A responsabilidade civil dos agentes bancários e financeiros, ao contrário da tradicional sistemática adotada pelo direito civil não decorre somente de ato culposo do agente causador da lesão, considerando que não é determinante a apuração da conduta do agente para a responsabilização. Portanto, o acidente de consumo causado por agente bancário ou financeiro trata-se da ocorrência de fato do produto ou serviço (EFING, 2000).

Quanto ao fato do serviço, o CDC estabelece que:

> Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos (BRASIL, 1990)

Assim, conforme aponta Efing (2000), se o serviço de gerenciamento da conta bancária prestado pela a instituição fornecedora é danosa e não pode oferecer a segurança, repercutindo esse dano na oferta de crédito, na imagem ou na segurança patrimonial do consumidor, resta configurado o fato do serviço bancário ou financeiro.

Nesse sentido, quanto à proteção dos dados pessoais, o Decreto nº 7.962, de 15 de março de 2013, estabelece que é responsabilidade do fornecedor, utilizar de mecanismos de segurança para o tratamento de dados do consumidor, sob pena de imposição de sanções:

> Art. 4º Para garantir o atendimento facilitado ao consumidor no comércio eletrônico, o fornecedor deverá:
>
> [...]
>
> VII - utilizar mecanismos de segurança eficazes para pagamento e para tratamento de dados do consumidor(BRASIL, 2013).

> Art. 72. Impedir ou dificultar o acesso do consumidor às informações que sobre ele constem em cadastros, banco de dados, fichas e registros:
>
> Pena Detenção de seis meses a um ano ou multa.
>
> Art. 73. Deixar de corrigir imediatamente informação sobre consumidor constante de cadastro, banco de dados, fichas ou registros que sabe ou deveria saber ser inexata(BRASIL, 2013)

Considerando que a implementação do *Open Banking* tem como fundamento a proteção dos dados pessoais, em caso de violação deverão ser observadas as regras de responsabilidade estabelecidas na LGPD. Assim, a referida lei considera que o tratamento de dados pessoais será considerado irregular na seguinte hipótese:

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

No que diz respeito às normas de responsabilidade, a LGPD estabelece que o controlador e operador de dados, no exercício de suas atividades de tratamento serão obrigados a reparação do dano, nos seguintes termos:

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

Dessa forma, os agentes de tratamento respondem solidariamente quando causarem dano patrimonial, moral, individual ou coletivo, podendo também responsabilizados por omissão, quando deixarem de adotar as medidas de segurança previstas na legislação, em casos de violação da segurança por terceiros, dando causa aos danos.

Contudo, se os danos ocorreram por culpa exclusiva do titular dos dados ou de terceiros; se não foi verificado nenhuma violação à legislação de proteção de

dados ou quando provarem que não realizaram o tratamento a eles atribuídoos agentes de tratamento poderão ser eximidos da responsabilidade.

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

Ademais, quando a violação do direito ocorrer no âmbito das relações de consumo, as regras de responsabilidade serão sujeitas ao CDC.

Além sujeição às regras de responsabilidade civil nos contratos financeiros e bancários, o BACEN estabeleceu na Resolução n°4.658/2018 medidas punitivas em caso de desobediência por parte dos atores de mercado com relação aos controles internos impostos à segurança cibernética:

> Art. 27. O Banco Central do Brasil poderá vetar ou impor restrições para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem quando constatar, a qualquer tempo, a inobservância do disposto nesta Resolução, bem como a limitação à atuação do Banco Central do Brasil, estabelecendo prazo para a adequação dos referidos serviços (BRASIL, 2018).

Em geral, as relações bancárias são ajustadas por meio de contratos de adesão, sendo regidas pelas normas do CDC. Contudo, devidos às reconfigurações de negócios e produtos bancários, a migração dos serviços bancários para as plataformas digitais acaba por transferir a responsabilidade para os usuários. Dessa forma, é preciso que haja maior atenção dos órgãos reguladores, e também dos clientes, no que diz respeito à regulação e contratação dos novos serviços e negócios bancários que estão surgindo.

Considerações finais

O compartilhamento de informações e dados no âmbito do direito bancário é uma prática recorrente no sistema financeiro brasileiro. Contudo, foi com a expedição do Comunicado nº 33.455, de 24 de abril de 2019, que o Banco Central do Brasil posicionou-se sobre a necessidade de regulação da prática e apresentou diretrizes para a implementação do *Open Banking* no Brasil.

Sob o viés das instituições financeiras, o *Open Banking* pode ser considerado um instrumento de personalização dos serviços ofertados ao consumidor. Em contrapartida, proporcionará ao cliente maior controle e gerenciamento de sua vida financeira, uma vez que terá o poder de decisão com quem irá compartilhar seus dados pessoais e terá acesso aos serviços que julgar mais vantajoso.

Contudo, conforme exposto ao longo do texto, é necessário considerar os dados pessoais, no contexto da prática do *Open Banking,* sob dois aspectos: na qualidade de um insumo econômico e também como bem jurídico a ser tutelado. Logo, é impossível desvincular o *Open Banking* de uma política de proteção e privacidade de dados, uma vez que à proteção desses dados está exposta aos diversos riscos.

Assim, a identificação desses riscos permite reflexão sobre o papel do Direito para regulação da abertura e, consequentemente, da proteção dos dados bancários/pessoais, considerando harmonicamente os princípios de livre mercado, controle informacional e proteção da privacidade.

Portanto, Bioni foi assertivo ao considerar que acapacidade e velocidade de inovação do cenário financeiro, demanda do ordenamento jurídico nacional mecanismos de regulação ágeis e, mesmo transitórios, eficazes. Caso isso não ocorra, poderá surgir imensa insegurança jurídica no país, violações aos direitos e ao mesmo tempo uma diminuição no potencial de inovação de negócios.

Dessa forma, um dos principais desafios à implementação do Open Banking diz respeito à dicotomia entre a entre a contemporânea economia de dados e as demandas normativas acerca da proteção de dados pessoais, de forma que haja incentivo ao desenvolvimento econômico e inovação tecnológica, porém com garantia da privacidade e outros direitos fundamentais, de forma a combater a assimetria informacional e de poder, bem como a vulnerabilidade do cidadão.

Logo, de acordo com o que apontam a doutrina, os relatórios técnicos e legislações, confirma-se a hipótese de que mesmo que haja pretensões normativas de garantir aos usuários das instituições financeiras à proteção de seus dados, haverá a dicotomia entre o desenvolvimento econômico e proteção de dados.

Referências Bibliográficas

BIONI, Bruno. Xeque-Mate: **O Tripé da Proteção de Dados Pessoais no Jogo de Xadrez das Iniciativas Legislativas no Brasil**, 2015. Disponível em: <http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf.>Acesso em: 13 jun. 2019.

_____, Bruno. **Dados Pessoais: Repensando o consentimento**. Jota. 24.12.2018. Disponível em:<https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/dados-pessoais-repensando-o-consentimento-24122018> Acesso em: 26 jun. 2019.

BELLINETTI, Luiz Fernando. **Limitações legais ao sigilo bancário.** Revista de Direito do Consumidor, v. 18, abr./jun. 1996. CAMPOS, Diogo Leite de. O sigilo bancário, Revista do Instituto dos Advogados de Minas Gerais, Belo Horizonte, n. 3, 1997.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Disponível em:<http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Acesso em: 13 jun. 2019.

_____. Banco Central do Brasil. **Comunicado n. 33.455, de 24 de abril de 2019**. Disponível em:<https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=33455>. Acesso em: 08 de jun. de 2019.

_____. Banco Central do Brasil. **Resolução n. 3.401, de 06 de outubro de 2006**. Dispõe sobre a quitação antecipada de operações de crédito e de arrendamento mercantil, a cobrança de tarifas nessas operações, bem como sobre a obrigatoriedade de fornecimento de informações cadastrais. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=33455>. Acesso em: 08 de jun. de 2019.

_____. Banco Central do Brasil. **Resolução n. 4.658, de 26 de abril de 2018**. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. Disponível em:<https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=33455>. Acesso em: 08 de jun. de 2019.

_____. **Decreto n. 7.962 de 15 de março de 2013.** Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico. Disponível em: <http://www.planalto.gov.br/Ccivil_03/leis/LCP/Lcp105.htm>. Acesso em: 13 jun. 2019.

_____. **Lei Complementar n. 105 de 10 de janeiro de 2001.** Brasília: Distrito Federal. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Disponível em: <http://www.planalto.gov.br/Ccivil_03/leis/LCP/Lcp105.htm>. Acesso em: 14 jun. 2019.

_____. **Lei Complementar n. 166 de 08 de abril de 2019.** Brasília: Distrito Federal. Altera a Lei Complementar nº 105, de 10 de janeiro de 2001, e a Lei nº 12.414, de 9 de junho de 2011, para dispor sobre os cadastros positivos de crédito e regular a responsabilidade civil dos operadores. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/lcp/Lcp106.htm>. Acesso em: 14 jun. 2019.

_____. **Lei Ordinária n. 8.078 de 11 de setembro de 1990.** Brasília: Distrito Federal. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>Acesso em: 13 jun. 2019.

_____. **Lei Ordinária n. 12.414 de 09 de junho de 2011**. Brasília: Distrito Federal. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>Acesso em: 13 jun. 2019.

_____. **Lei Ordinária n. 12.965 de 24 de abril de 2014.** Brasília: Distrito Federal. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>Acesso em: 13 jun. 2019.

_____. **Lei Ordinária n. 13.709 de 14 de agosto de 2018.** Brasília: Distrito Federal. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>Acesso em: 15 jun. 2019.

CAMPOS, Diogo Leite de. **O sigilo bancário.** Revista do Instituto dos Advogados de Minas Gerais, Belo Horizonte, n. 3, 1997. p. 210

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006, p. 161-162.

_____, Danilo. **A proteção dos dados pessoais como um direito fundamental.** Espaço Jurídico. Joaçaba, v. 12, n. 2, jul./dez. 2011.

EFING, Antônio Carlos. **Contratos e procedimentos bancários à luz do Código de Defesa do Consumidor.** 1. ed., 3. tir. São Paulo: Revista dos Tribunais, 2000. p. 31.

ESTEVES, Jean Soldi. **A responsabilidade civil nos contratos bancários**. 2008. 211 f. Dissertação (Mestrado em Direito) - Pontifícia Universidade Católica de São Paulo, São Paulo, 2008.

FEBRABAN. **Pesquisa FEBRABAN de tecnologia bancária 2019**. 2019. Disponível em: <https://cmsportal.febraban.org.br/Arquivos/documentos/PDF/Pesquisa-FEBRABAN-Tecnologia-Bancaria-2019.pdf>Acesso em: 17 jun. 2019.

GOETTENAUER, C. **Regulação Responsiva e a Política de Segurança Cibernética do Sistema Financeiro Nacional.** Revista de Direito Setorial e Regulatório, Brasília, v. 5, n. 1, p. 131-146, maio 2019.

HUNGRIA, N.; LACERDA, R. C. **Comentários ao Código Penal.** 4. ed. Rio de Janeiro: Ed. Revista Forense, 1980.

PTI - Profissionais TI. **Pesquisa Nacional de Segurança da Informação: Divulgação dos resultados!** Disponível em: <https://www.profissionaisti.com.br/2014/11/pesquisa-nacional-de-seguranca-da-informacao-divulgacao-dos-resultados> Acesso em: 11 out. 2019.

PCW. **Pesquisa Fintech Deep Dive 2018**, 2018. Disponível em:<https://www.pwc.com.br/pt/setores-de-atividade/financeiro/2018/pub-fdd-18.pdf> Acesso em 12 jun. 2019.

SIMÕES, L. A.; FERREIRA, L. E. M.; FERREIRA, F. M. **O que é Open Banking?** São Paulo, 16 de abril de 2019. Disponível em:<https://baptistaluz.com.br/institucional/o-que-e-open-banking/>Acesso em 13 jun. 2019.

TAVARES, P. S. A.. **Regulação e Auto-regulação do Mercado de Capitais.** Âmbito Jurídico, v. 79, p. 8260, 2010. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=8260> Acesso em 12 jun. 2019.

VALENTE, Christiano MW. **Sigilo Bancário: Obtenção de Informações pela Administração.** Tributária Federal. Rio de Janeiro: Editora Lúmen Juris, 2006.

WINTER, Estéfano Luís de Sá. **O novo ecossistema de serviços financeiros.** Rumos. Rio de Janeiro: ABDE, v. 292, pp. 32-33, 2017.