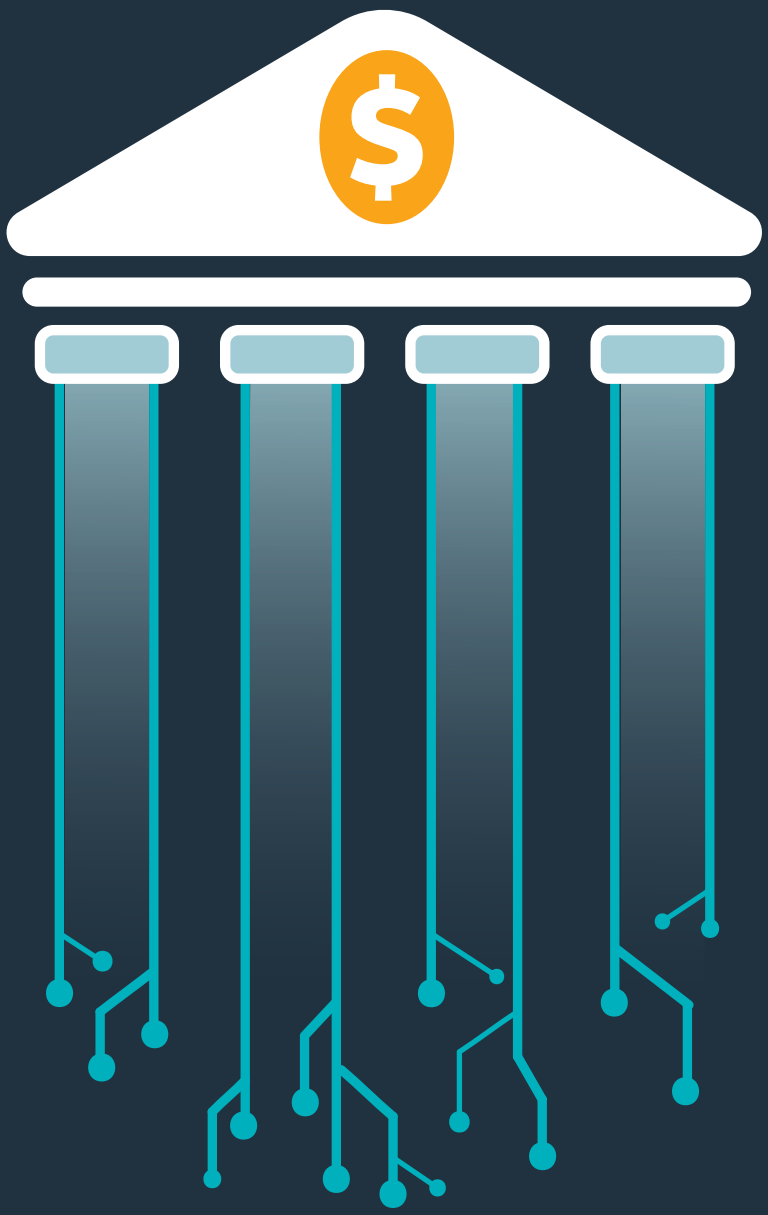
LAPIN

RELATÓRIO

Open Banking & LGPD

Entraves e Eficiências



LAPIN

LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET

Apoio:

CITTADINO, CAMPOS & ANTONIOLI

ADVOGADOS ASSOCIADOS

O objetivo do presente Relatório é produzir um estudo detalhado sobre a interlocução entre a Lei Geral de Dados Pessoais (LGPD) e o Open Banking para empresas, agentes públicos e consumidores brasileiros. Dessa forma, o documento aborda (I) as eficiências e os entraves da conformidade com a LGPD para empresas de crédito digital, (II) soluções jurídicas sobre adequação com a LGPD de forma específica para o mercado de crédito digital e (III) formas de compatibilidade da LGPD com demais normas para prevenção e contenção de futuros custos.

O Relatório foi dividido em cinco seções. A primeira seção apresenta a estrutura e o funcionamento do Open Banking, especificando o seu histórico e contexto, a atuação dos agentes envolvidos nesse tipo de relação e os tipos dados transacionados. Já a segunda seção expõe o histórico da Lei Geral de Proteção de Dados (LGPD) e de que forma ocorre sua aplicação no modelo do Open Banking. A terceira seção apresenta os desafios de implementação do Open Banking em relação à LGPD e às normas em vigor relativas ao Sistema Financeiro Nacional (SFN). Por conseguinte, a quarta seção demonstra os entraves e as eficiências da adoção do Open Banking pelo setor privado. A quinta seção define as hipóteses obrigatórias de transferência de dados por pessoas a bancos à luz da LGPD.

Laboratório de Políticas Públicas e Internet (LAPIN)

Coordenação: Gabriel Souto

Revisão: Amanda Espiñeira e Thiago Moraes

Escritores: Alexandra Krastins, Felipe Silva, Fernando Fellows, Lucas Madriles e Sarah Fernandes

Design: Bruna Nascimento e Luís Felipe (Lamparina Design)

Sumário

5 Introdução

6 Introdução ao Open Banking

7 O que é o Open Banking?

8 Quais os benefícios do Open Banking

8 O que é o PSD2?

10 A Lei Geral de Proteção de Dados e o Open Banking

11 Breve histórico dos diretos à privacidade e da proteção de dados no mundo

14 Conceitos Gerais

18 Dados pessoais financeiros

19 As intersecções entre a Lei Geral de Proteção de Dados e o Open Banking

21 A aplicabilidade dos princípios da qualidade dos dados, transparência e não discriminação da LGPD

30 Quais os desafios de implementação do Open Banking frente à LGPD e regulações do BCB?

25 Os limites para o consentimento

27 Segurança Cibernética

28 O Open Banking e a cooperação entre Autoridades

30 Quais as eficiências e os entraves econômicos para as empresas que adotarem o Open Banking?

31 O posicionamento do sistema bancário brasileiro

33 A desconfiância do setor bancário tradicional ao Open Banking

34 As oportunidades do Open Banking ao setor bancário

35 Riscos do Open Banking ao sistema financeiro

39 Conclusão

40 Referências

Introdução

A relação de confiança e responsabilização estabelecida por contratos bancários de adesão não é suficiente para solucionar as preocupações quanto ao processamento de dados financeiros. Isso se deve a relação *business-to-consumer* (B2C) entre banco e cliente, que é permeada por assimetria informacional. O processamento, armazenamento, distribuição, arquivamento e eventual eliminação de dados financeiros têm um alto custo de monitoramento pelo cliente, uma vez que ele despenderá recursos pela busca da informação quanto ao paradeiro de seus próprios dados. O alto custo ocorre pela importância dos dados que, além do seu papel na economia digital, são infinitamente utilizáveis, diferenciando de outras mercadorias de uma maneira fundamental. Os mesmos dados podem ser usados simultaneamente, sem serem esgotados, pelas mais variadas instituições e empresas. Assim, quanto maior o acúmulo de dados e maior a capacidade de processamento deles, maior é o poder informacional da empresa. Nesse sentido, embora ainda pouco discutido, é fato que alguns bancos vendem dados de clientes a terceiros[1].

Nesse contexto surge o Open Banking, em português Sistema Financeiro Aberto, que é um modelo de compartilhamento padronizado de dados e serviços no qual dados bancários são compartilhados com o consentimento de seu titular. Isso ocorre através de infraestruturas informáticas interoperáveis, beneficiando os consumidores com soluções mais eficientes e inovadoras através de uma maior concorrência. Eles poderão, por exemplo, ver todas as suas finanças em um só aplicativo ou poderão obter produtos e serviços personalizados e/ou com desconto, com base em seu perfil financeiro. Dessa forma, o consumidor tem mais controle sobre o que fazer e o que fazem com os seus dados, o que é chamado de "economia das informações pessoais".

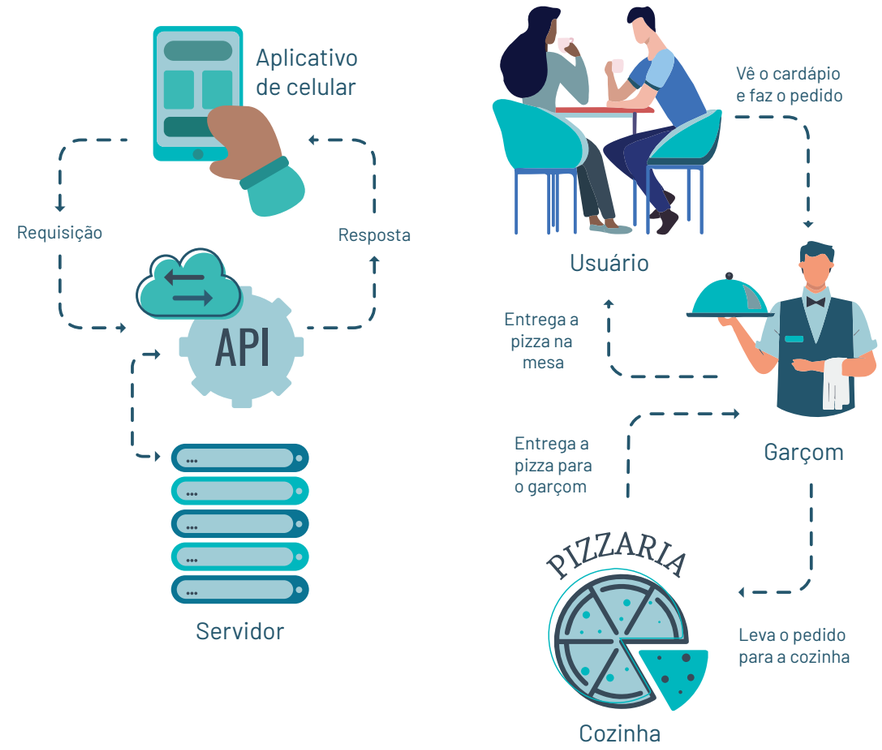
Introdução ao Open Banking

Após pesquisas no Reino Unido, sobre a melhoria nos serviços de conta corrente prestados a pessoas físicas, e também a pequenas e médias empresas, concluiu-se que deveria existir uma renovação nos serviços bancários e financeiros. Diversas modificações foram propostas, as quais acreditava-se que poderiam favorecer a ampliação da concorrência e escolha, e uma destas modificações foi o Open Banking[2].

O que é o Open Banking?

O Open Banking representa a transformação digital nos serviços financeiros, pois visa proporcionar a prestação de serviços diferentes e inovadores, enquanto provê maior controle aos consumidores em relação às suas finanças e informações. Isso é possível de ser atingido por meio da obrigatoriedade de bancos e instituições financeiras tornarem certas informações acessíveis a outras instituições reguladas, de uma forma padronizada, segura e expressamente consentida.

O compartilhamento de dados por bancos e instituições financeiras é possibilitado por APIs (*Application Programming Interfaces*), em português, interfaces de programação de aplicações. Atualmente, os sistemas não funcionam individualmente, mas precisam de outros integrados para atingir sua potencialidade. Uma API tem como objetivo disponibilizar recursos de uma aplicação para uso em outra, com restrições de acesso a informações e recursos, seguindo regramentos específicos. Trata-se de uma forma pela qual diferentes aplicações possam se comunicar através de uma rede, utilizando uma linguagem compreendida por ambas[3].



Portanto, o Open Banking consiste na padronização de APIs, para a interoperabilidade entre sistemas que bancos e instituições financeiras utilizam para pagamentos e acesso à informação. Assim, aplicativos e websites de qualquer empresa devidamente regulamentada poderão se comunicar com os bancos, através de metodologia estandardizada, para oferecer diversos novos serviços.

Quais os benefícios do Open Banking?

Inicialmente, o Open Banking facilita aos consumidores a informação e comparação de detalhes de contas correntes e outros serviços financeiros. Como vantagens do Open Banking trazidas para **consumidores**, podemos elencar: (I) gerenciamento financeiro, através de ferramentas que demonstram como o dinheiro é gasto e de onde provém, para identificar formas de economizar; (II) visão única de diversas contas em uma mesma plataforma; (III) ferramentas de gerenciamento de dívidas, com alertas e recomendações para produtos que podem ajudar na escolha por menores taxas de juros.

Além disso, o Open Banking traz benefícios aos pequenos negócios, entre outros: (I) ferramentas para gerenciamento de fluxo de caixa e auxilio em contas, que ajudam na escolha por menores taxas de juros; (II) ferramentas para auxiliar na contratação de empréstimos. Diante dessas vantagens, a União Europeia decidiu regulamentar o Open Banking e o fez por meio do chamado PSD2.

O que é o PSD2?

A Diretiva Revisada de Serviços de Pagamento da União Europeia[4] (PSD2) publicada em 2016, é a regulação que modernizou a diretiva já existente desde 2009, sobre pagamentos nos países europeus, e trouxe medidas relativas ao Open Banking para permitir aos consumidores e pequenas empresas da Europa terem maior controle de suas informações financeiras. Resumidamente, a PSD2 visou promover uma maior eficiência no mercado de pagamentos da União Europeia (UE), bem como a concorrência em um ambiente em que *players* como *fintechs* e uma nova geração de produtos de pagamento e serviços estão surgindo[5].

Ressalta-se que a PSD2 possui efeitos extraterritoriais, já que é aplicável para operações financeiras ainda que apenas um dos prestadores de serviços de pagamento esteja situado na União Europeia, independentemente da moeda utilizada. Em paralelo à reforma iniciada na União Europeia, que viria a culminar na PSD2, o governo do Reino Unido estabeleceu a criação do Open Banking Working Group (OBWG)[6], para a criação de um *framework* de desenvolvimento de padrões API aplicáveis aos bancos.

Além de existirem regulações específicas para o Open Banking na Europa com todo todo um arcabouço propício para o desenvolvimento desse modelo financeiro, entender a proteção de dados pessoais é essencial nesse sistema, uma vez que sua base se encontra amparado em dados. Esse modelo também é realidade em outras regiões e países, como no Brasil. Assim, apresenta-se nos próximos tópicos uma discussão introdutória sobre proteção de dados pessoais, a Lei brasileira que trata do tema e sua relação com o Open Banking.

A Lei Geral de Proteção de Dados e o Open Banking

Há poucos anos, tópicos que traziam à tona assuntos relacionados à privacidade e proteção de dados pessoais eram tratados de forma residual no Brasil. Antes da Lei Geral de Proteção de Dados (Lei Federal 13.709/2018), o que se tinha no país eram leis esparsas que tratavam da privacidade e proteção de dados de forma pontual, principalmente, no âmbito de mercados regulados, como o mercado financeiro.

Com a avanço da tecnologia e do fluxo de informações, instituições públicas - e os cidadãos - viram crescer cada vez mais a importância de tecer normas e diálogos relacionados à privacidade de dados pessoais, e, principalmente, de trazer o indivíduo, detentor dos dados, ao centro das discussões, assim como demonstrar seu protagonismo como dono de seus dados.

Breve histórico dos direitos à privacidade e da proteção de dados no mundo

O direito à privacidade está presente na Declaração Universal dos Direitos Humanos de 1948. O artigo 12º da DUDH dispõe que "Ninguém será sujeito a interferências em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataques à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques." [7]

A proteção da privacidade começou a ganhar atenção após as atrocidades cometidas na Segunda Guerra Mundial, por parte do governo alemão nazista. Durante os anos de 1933 a 1945, a população alemã foi controlada pelo regime nazista, por meio de um monitoramento constante. Durante o terceiro Reich, o governo manteve o "índice de judeus", o qual listava a identidade de todos os judeus desde a geração dos seus avós. Além disso, o governo utilizou dados coletados durante a República de Weimar, incluindo dados de homossexuais.[8]

De acordo com Alvar Freude e Trixy Freude em "*Echoes of History: Understanding German Data Protection*", a perseguição da Alemanha nazista a judeus e homossexuais provou que, independentemente da intenção da entidade de coleta de dados, a coleta de informações pessoais sobre indivíduos pode ser perigosa por si só.

Com o desenvolvimento tecnológico durante a década de 1960, o conceito de privacidade passou a ser atrelado à coleta de dados por meio da rede de computadores. Sendo assim, devido às perversidades cometidas na Segunda Guerra e ao desenvolvimento do cenário computacional, a Europa foi pioneira na discussão e implementação de leis que protegiam informações dos indivíduos. Desenvolveu-se, assim, o conceito de **autodeterminação informacional**, a esfera positiva do direito à privacidade. Este conceito passou a ser reconhecido como o direito à proteção de dados pessoais. A primeira lei estadual acerca da proteção de dados pessoais surgiu no estado alemão de Hesse, na década de 1970. Já em 1974, seguiu-se o estado da Renânia-Palatinado; e em 1977, a Lei Federal Alemã de Proteção de Dados foi aprovada.[9]

Antes mesmo da Lei Federal Alemã, foi aprovada na Suécia, em 1973, a primeira lei nacional de proteção de dados da história. Assim como a Lei de Hesse, o Ato de Dados Sueco tratava de forma genérica a proteção de dados pessoais, não abarcando as situações que a coleta de dados poderia ocorrer, por exemplo. Entretanto, foi um marco ao trazer o tema para a agenda governamental.[10]

Diversos países europeus seguiram o mesmo movimento e criaram suas próprias legislações de proteção de dados, como a França, Alemanha e Dinamarca. Uma década após a instituição da primeira lei estadual em Hesse, em 1981, foi estabelecida a Convenção 108, o primeiro marco legal transnacional de proteção de dados. Esta considerava que era necessário ampliar a proteção dos direitos e liberdades das pessoas, considerando o respeito à vida privada, devido ao fluxo crescente de dados pessoais através das fronteiras.[11]

Após 25 anos do nascimento da Lei de Hesse, em 1995, foi promulgada a Diretiva 95/46/CE, a qual tratava sobre o direito à privacidade e proteção de dados de todos os países membros do bloco da União Europeia, estabelecendo uma legislação em comum. A Diretiva vigorou até 2018, quando foi substituída pela *General Data Protection Regulation*,

conhecida como GDPR. A regulação europeia trata do fluxo de dados existentes nos países membros e possui alcance extraterritorial a todos os países do mundo que tratam dados do mercado europeu.

Saindo do contexto europeu, no Brasil também houve debate sobre o assunto de proteção de dados durante a década de 1970. Entretanto, o Congresso rejeitou uma iniciativa em 1978 de proposta de uma lei que regulasse a proteção de dados pessoais, e mais duas em 1984. Somente com a pressão de organismos internacionais na metade dos anos 2000 que o governo brasileiro inseriu a discussão do assunto na pauta do Congresso.

A primeira iniciativa acatada pelo Congresso foi o Comitê Gestor da Internet no Brasil, em 2009, que publicou dez princípios do uso da rede.[12] O primeiro tratava da privacidade do indivíduo e respeito aos direitos humanos. Um ano depois, em 30 de novembro de 2010, o Ministério da Justiça abriu a Primeira Consulta Pública sobre o chamado "Anteprojeto de Lei de Proteção de Dados Pessoais", o qual teve participação de diversos setores da sociedade, principalmente do setor privado. O primeiro projeto de lei foi apresentado em 13 de junho de 2012, pelo deputado federal Milton Monti[13], tendo como fonte de inspiração a consulta pública realizada pelo Ministério da Justiça.

A discussão sobre proteção de dados somente se intensificou no Brasil em 2013, durante o governo Dilma, após as revelações de Edward Snowden sobre a espionagem do governo norte-americano. A repercussão do caso impulsionou o governo a aprovar em 24 de abril de 2014 o Marco Civil da Internet[14]. Já no ano de 2015 foram retomadas as discussões sobre o anteprojeto, com a realização de uma segunda consulta pública. Esta trouxe um contingente maior de contribuições, as quais deram origem ao PL 5276/16. Este foi protocolado e encaminhado à Câmara dos Deputados em 12 de maio de 2016, um dos últimos atos de Dilma como presidente.

Em 26 de Outubro de 2016, foi criada a Comissão Especial de Proteção de Dados Pessoais[15], presidida pela deputada Bruna Furlan (PSDB). Em dezembro do mesmo ano, a Comissão realizou a primeira audiência pública sobre o tema, com a participação da sociedade civil, academia, setor privado e governo. Mais 11 audiências públicas e 2 Seminários Internacionais foram realizados até julho de 2017, com o objetivo de ajudar "os atores envolvidos a depurar o entendimento sobre diversos conceitos ligados à Proteção de Dados"[16]. Até o início de 2018, a perspectiva de aprovação do projeto de lei era baixa. Entretanto, de acordo com o observatório do Data Privacy BR[17], uma série de acontecimentos ao longo do ano mudaram este cenário, fazendo com que a LGPD fosse aprovada, sendo eles:

I Escândalo da Cambridge Analytica com a revelação do uso de dados de usuários do Facebook em propagandas eleitorais dos Estados Unidos e na saída do Reino Unido da União Europeia, o que trouxe uma preocupação mundial acerca da privacidade individual e tratamento de dados;

II Ingresso do Brasil na Organização para Cooperação e Desenvolvimento Socioeconômico (OCDE), a qual exige a regulamentação de dados pessoais;

III Entrada em vigor da GDPR em maio, influenciando os países que mantêm contato com o continente europeu a se preocuparem com segurança jurídica de dados;

IV Exigência da aprovação do PL 5276 por articulação na Câmara dos Deputados, para tramitação do Cadastro Positivo;

V Enfraquecimento do Executivo frente ao legislativo, devido às acusações de corrupção contra Temer; e

VI Aproximação da Copa do Mundo de 2018 e eleições presidenciais, tornando o prazo para aprovação mais curto;

Após pressão do contexto social e de entidades civis, bem como várias deliberações do Congresso, em 29 de maio de 2018 o PL nº 5276/16 foi aprovado pela Câmara dos Deputados, seguindo então para o Senado Federal, onde teve sua denominação alterada para Projeto de Lei da Câmara nº 53 de 2018[18].

Em julho de 2018, o Projeto foi colocado em pauta na Comissão de Assuntos Econômicos do Senado, sendo aprovado por unanimidade em 10 de julho de 2018. A Lei Federal sob nº 13.709 foi sancionada pelo poder Executivo um mês depois, em 14 de agosto de 2018, com alguns vetos, principalmente a respeito da constituição da Autoridade Nacional de Proteção de Dados (ANPD), autoridade supervisora da aplicação da LGPD, e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade.

Neste sentido, em dezembro de 2018, o presidente Michel Temer expediu a Medida Provisória (MP) 869/2018 que, além de realizar alterações pontuais no texto da Lei nº 13.709[19], incluiu a ANPD na estrutura da Presidência da República, estabelecendo sua composição, suas competências e garantindo sua autonomia técnica.

A MP deu origem à Lei nº 13.853 de 2019[20], a qual estabelecia a vigência dos dispositivos da LGPD (exceto os itens relacionados à ANPD e ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade) para agosto de 2020. Entretanto, com a declaração da pandemia de COVID-19[21] em março do ano de 2020 o cenário mudou. Um mês após a declaração da pandemia da OMS, foi apresentado um Projeto de Lei (PL 1.179/2020)[22] visando prorrogar as sanções da LGPD para agosto de 2021, elaborado pelo Deputado Enrico Misasi (PV-SP). Ademais, algumas semanas depois, em 29 de abril, o presidente Jair Messias Bolsonaro publicou a MP 959/2019[23], estabelecendo a operacionalização do benefício emergencial devido aos impactos econômicos causados pela pandemia do COVID-19, além de alterar o artigo 65º da LGPD, adiando sua vigência para 3 de maio de 2021.

Em 03 de abril de 2020, o PL 1.179/20 foi aprovado pelo Senado Federal, prorrogando a vigência da LGPD para janeiro de 2021 e a aplicabilidade das sanções administrativas para agosto de 2021. Entretanto em 14 de maio de 2020, os deputados decidiram remover do texto original do PL 1.179/20 a parte em que se postergava a vigência dos artigos restantes da LGPD. Entretanto, para que não houvesse conflito com a MP 959/2020 ficou mantida a entrada em vigor dos artigos relacionados às sanções para 01 de agosto de 2021. Em 19 de maio de 2020, o Senado Federal aprovou definitivamente o texto substitutivo da Câmara dos Deputados ao PL 1179/2020. Em 18 de setembro de 2020, a Lei Geral de Proteção de Dados (LGPD) entrou em vigor.

Conceitos Gerais

A Lei Geral de Proteção de Dados, seguindo o modelo europeu da GDPR, regula o tratamento de dados pessoais, realizado por pessoa natural ou por pessoa jurídica de direito público ou privado, com o fim de resguardar os direitos fundamentais da liberdade, da privacidade e do livre desenvolvimento da personalidade da pessoa natural.[24]

Ainda não existe na Constituição Federal um direito fundamental expresso, relacionado à proteção de dados pessoais; não obstante, a LGPD pautou seu escopo principalmente no artigo 5º, inciso X, da Constituição de 1988[25], que garante aos brasileiros e estrangeiros residentes no País o direito à intimidade, à vida privada e à liberdade.

Assim, a intenção da LGPD é trazer ao ordenamento jurídico e constitucional disposições e diretrizes que tratam acerca de quaisquer operações realizadas com dados pessoais, seja por controladores ou operadores (agentes de tratamento)[26], como:

> A coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.[27]

O escopo de aplicação da Lei será melhor explicado a seguir.

Escopo de aplicação da LGPD

Além do conceito de tratamento dos dados pessoais, um ponto importante a ser analisado antes de adentrarmos mais afundo nos conceitos da LGPD, se refere à aplicabilidade desta. A Lei, no começo do texto, em seu artigo 3º já delimita a quais operações de tratamento se aplica. Independente do meio, do país da sede da pessoa física ou jurídica, ou onde estejam localizados os dados, a LGPD aplica-se a:

I operações realizadas no território brasileiro;

II operações que tenham por objetivo a oferta ou o fornecimento de bens ou serviços ou tratem dados pessoais de indivíduos localizados em território nacional; ou

III a operações em que os dados pessoais tenham sido coletados no território nacional.

Os requisitos não são cumulativos, o que significa que basta se encaixar em apenas um requisito que a LGPD já terá sua aplicabilidade efetiva, com ressalvas às disposições do art. 4º[28], que delimita hipóteses em que a lei não se aplica.

Caso uma pessoa física ou jurídica realize o tratamento de um dado pessoal a partir de quaisquer das operações definidas no artigo 5º, inciso X, da LGPD, e este tratamento se encaixe em qualquer uma das hipóteses mencionadas no parágrafo anterior, a LGPD será aplicada. Dessa forma, mesmo que uma companhia dos EUA colete e armazene dados pessoais em um servidor na Suíça, caso este tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou tratem dados pessoais de indivíduos localizados em território nacional, a LGPD se aplicará à companhia.

Bases legais para tratamento de dados

Além da aplicabilidade da LGPD, outro tema de grande relevância é apresentado no artigo 7º da Lei. Neste dispositivo legal são exploradas as hipóteses, ou bases legais, que justificam o tratamento dos dados pessoais; hipóteses essas taxativas, uma vez que o tratamento de dados pessoais por um controlador (pessoa natural ou jurídica que toma decisões em relação ao tratamento dos dados pessoais) e/ou operador (trata dados a partir das ordens do controlador) só poderá ser realizado se for baseado em uma das conjecturas legais dispostas na LGPD ou em outra norma legal ou regulatória.

A correta aplicação das bases legais ao tratamento de dados pessoais pelas instituições financeiras implicará diretamente na eficiência e qualidade das informações circuladas no mercado financeiro. Assim, instituições financeiras e órgãos reguladores deverão trabalhar de forma harmônica e em conjunto acerca do correto uso das hipóteses dispostas na legislação. O *Guideline* de Proteção de Dados para Serviços Financeiros Regulados na União Europeia, elaborado pelo *European Data Protection Supervisor* (EDPS) é bem incisivo em recomendar que qualquer ato que envolva o processamento de dados pessoais deve basear-se em uma análise adequada da hipótese legal para o processamento e, quando necessário e aplicável, essa hipótese deve ser especificada em instrumento legal objeto do tratamento[29].

Principalmente **sob a ótica do Open Banking**, segundo a LGPD, dentre outras hipóteses, o tratamento de dados pessoais poderá ser realizado[30] quando o titular consentir ou, sem o seu consentimento, nas seguintes hipóteses:

I quando for necessário para cumprir obrigação legal ou regulatória;

II quando necessário para a execução de contrato ou de procedimentos preliminares, quando o titular dos dados for parte ou a seu pedido;

III para o exercício regular de direitos em processo judicial, administrativo ou arbitral;

IV para atender a interesses legítimos do controlador ou de terceiros, resguardados os direitos e liberdades fundamentais do titular; e

V para a proteção do crédito.

Ainda, a Lei estabelece algumas hipóteses específicas para o tratamento de dados sensíveis, que são dados que revelam aspectos mais íntimos do titular de dados e podem causar uma exposição social e/ou política não desejada, evidenciando processos discriminatórios de tratamento. Por isso, dados enquadrados como sensíveis demandam proteção e controles específicos por parte do controlador e do operador de dados pessoais. A LGPD estabeleceu as seguintes categorias de dados sensíveis:

> dados sobre a 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.[31]

Para tratar dados sensíveis, o artigo 11 da LGPD delimita que este poderá ocorrer, em regra, apenas com o consentimento específico e destacado do titular, devendo o tratamento ser realizado para finalidades específicas. O consentimento específico e destacado refere-se à manifestação particular e definida do titular para determinado tratamento, a partir de uma declaração de vontade clara e ressaltada. O racional do artigo reforça a necessidade de ser demonstrada a livre ciência do titular de forma inequívoca.

De acordo com as recomendações da *EPDS*[32], qualquer ação que resulte no tratamento de dados sensíveis deve ser clara sobre qual das hipóteses legais se aplicará. Assim, importante ressaltar que o tratamento de dados sensíveis poderá ser exercido sem o consentimento do titular, entretanto, apenas se enquadrado nas hipóteses do art. 11º, como para o cumprimento de obrigação legal ou regulatória, exercício regular de direitos, em contrato e em processos judiciais, administrativos e arbitrais, ou para prevenir fraudes e garantir a segurança do titular. Portanto, as hipóteses dispostas no art. 7º, fundamentadas em execução de contrato, interesse legítimo e proteção ao crédito, não amparam o tratamento de dados pessoais sensíveis.

Consentimento e o Open Banking

Para fins do presente relatório, vamos nos ater especialmente à **base legal do consentimento**, uma vez, que conforme artigo 8º da Resolução Conjunta nº 4.658/2018 do Banco Central do Brasil[33], grande parte do compartilhamento de dados, incluindo dados pessoais, carecem do consentimento de seus titulares.

O consentimento é a declaração livre e evidente pela qual o titular dos dados pessoais aceita o tratamento dos seus dados para uma finalidade específica.[34] Conforme a LGPD, consentimento é a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".[35] A manifestação livre refere-se à escolha do titular destituída de imposição ou constrangimento; a manifestação informada refere-se à escolha de consentir determinado tratamento, realizada pelo titular a partir de informações claras acerca deste e o conceito de manifestação inequívoca relaciona-se a uma ação positiva por parte do titular, que não deixe dúvidas acerca de sua intenção em consentir o tratamento de seus dados pessoais.

Assim, é direito do titular e a ele deve ser dada a liberdade de escolher acerca do tratamento dos seus dados, devendo esta escolha ser manifestada de forma clara, para finalidades específicas e informadas. Os requisitos da LGPD foram construídos para garantir ao titular o direito de escolher o que fazer com os seus dados, bem como cumprir com os fundamentos dispostos na LGPD, principalmente os relacionados à autodeterminação informativa, defesa do consumidor, dignidade e ao exercício da cidadania pelas pessoas naturais.[36]

Conforme a LGPD, caso, após obter o consentimento do titular, o controlador necessite compartilhar dados pessoais, deverá comunicar previamente ao titular acerca do novo tratamento e obter o seu consentimento para esta nova finalidade. Ainda, importante destacar que o ônus da prova em relação à coleta do consentimento caberá ao controlador dos dados pessoais, sendo, conforme a LGPD, proibido o tratamento de dados sob vício de consentimento.

Além do direito a manifestar - ou não - o seu consentimento, o titular dos dados possui outros direitos delimitados ao longo do texto da lei. Dentre eles, é mencionado um rol de direitos no Capítulo III da LGPD; direitos estes que advém dos princípios da liberdade, da intimidade e da privacidade.

De acordo com o texto, o titular tem o direito de **confirmar e acessar seus dados**, bem como **solicitar sua correção** quando estes estiverem incompletos, inexatos ou desatualizados, garantindo assim sua qualidade; pode **solicitar informações** sobre a possibilidade de não fornecer seu consentimento, assim como revogá-lo. Além disso, a LGPD possibilita que o titular faça a **portabilidade dos seus dados** a outro fornecedor de serviço ou produto, direito este que converge pontualmente com um dos objetivos do Open Banking.

Além de resguardar o controle do titular em relação a seus dados, grande parte dos direitos do titulares estabelecidos na LGPD possibilitam a adequação e melhoria do oferecimento de produtos e prestação de serviços aos indivíduos, uma vez que, como exemplo, o tratamento de dados completos, exatos e atualizados é fundamental para o funcionamento otimizado e orgânico do mercado de crédito, impactando diretamente o mercado financeiro e demais setores da economia.

Quais as hipóteses de transferência obrigatória de dados por pessoas a bancos?

O setor financeiro está sujeito a diversas normas setoriais, além da legislação brasileira como um todo. Pode ocorrer a transferência de dados financeiros por pessoas a instituições financeiras, tanto entre as instituições financeiras e os consumidores, bem como entre as próprias instituições financeiras.

As relações de troca de dados entre os consumidores e as instituições financeiras visa a finalidade de cumprimento da prestação de serviços financeiros, mas também pode embasar o cumprimento de obrigações das instituições financeiras perante auto-

ridades e órgãos reguladores.

Há situações em que as instituições financeiras tratam e compartilham dados dos consumidores em razão da necessidade de envio de informações relativas a atividades ilícitas ou abusivas, nos termos da legislação e regulamentações vigentes, sendo aplicados o art. 7º, II e o art. 11º, II, a da LGPD. Tais compartilhamentos podem ser feitos aos reguladores do setor, Banco Central do Brasil (BCB), Comissão de Valores Mobiliários (CVM) e Conselho de Controle de Atividades Financeiras (COAF). Como exemplos de situações que ensejam notificações obrigatórias e, portanto, compartilhamento de dados pessoais pelas instituições financeiras, há ações que trazem indícios de crimes contra o sistema financeiro nacional, conforme a Lei nº 7.492/1986, ou de lavagem de dinheiro, nos termos da Lei 9.613/1998.

Ainda, é lícito às instituições financeiras a troca de informações relativas aos consumidores com outras instituições financeiras, para composição de bases de dados, inclusive no que se refere à inadimplência, caso em que o Código de Defesa do Consumidor, em seu art. 43[37], disciplina a necessidade de transparência e direito de acesso e de correção ao consumidor, bem como estabelece requisitos para sua legalidade.

Sobre o tema, a Lei do Cadastro Positivo (12.414/2011) regulamenta a formação e obrigações relativas aos bancos de dados de histórico de crédito, alterada pela Lei Complementar 166/2019. Após a alteração, o acesso aos dados de consumidores foi ampliado e ficou estabelecida a possibilidade de inclusão de dados dos consumidores (*opt-in*) de forma automática e a sua exclusão (*opt-out*) por solicitação.

Aqui, poderia se visualizar uma contradição com a LGPD no que se refere ao consentimento, mas a LGPD prevê a base legal de proteção ao crédito[38] para justificar operações de tratamento de dados como essa. Dessa forma, eventual conflito jurídico talvez deva ser sanado pelas autoridades judiciárias competentes. Ademais, guias da ANPD poderiam auxiliar a estabelecer o ponto de equilíbrio entre as bases legais do consentimento e da proteção ao crédito.

Ressalta-se que as trocas de informações realizadas pelas instituições financeiras devem cumprir os requisitos de sigilo bancário[39], bem como de confidencialidade estabelecidos pelo Banco Central do Brasil e pela Comissão de Valores Mobiliários, respeitadas as exceções previstas pelo art. 1º da Lei 105/2001[40].

Dados pessoais financeiros

A LGPD apenas conceitua o que são dados pessoais e dados sensíveis, não especificando ao longo do texto o que seriam dados financeiros que, ao contrário do que muitas pessoas pensam, não se enquadram diretamente na categoria de dados sensíveis. Assim, dados financeiros, em regra, não são por si só dados sensíveis, entretanto estes podem facilmente se tornar dados sensíveis a depender do contexto e de sua relação com outros dados pessoais. Por exemplo, dados de transações de crédito de um indivíduo que indiquem a compra de um medicamento ou o pagamento de uma consulta podem ser considerados sensíveis, pois referem-se à saúde do indivíduo. Importante que o controlador de dados financeiros analise em que contexto esses dados serão considerados sensíveis, já que, conforme a LGPD, regras mais restritivas se aplicarão para o tratamento dessa categoria de dados.

Os dados financeiros já eram objeto de proteção antes da LGPD. A Lei do Sigilo Bancário[41], de 2011, e regulamentos do BCB, como a Resolução Conjunta nº 4.658/2018 do BCB[42], que dispõe sobre a política de segurança cibernética das instituições financeiras, já tratavam sobre os assuntos relacionados ao sigilo, confidencialidade e proteção de dados.

Considerando que na legislação não existe uma definição específica que delimite o termo "dados pessoais financeiros", o conceito será construído com base no racional da Lei do Sigilo Bancário, que em seu artigo 1º delimita que deverá ser protegido o sigilo das operações ativas e passivas das instituições financeiras, bem como seus serviços prestados. Assim, considerando os racionais dispostos, para os fins do presente relatório, iremos considerar dados pessoais financeiros como quaisquer informações referentes à pessoa natural identificada ou identificável (conforme direcionado pela LGPD) relacionadas a operações financeiras ativas e passivas, bem como serviços financeiros prestados.

A Resolução Conjunta nº 4.658/2018 do BCB[43] não conceitua dados pessoais financeiros. Entretanto, em seu artigo 5º, baliza os tipos de dados que serão compartilhados no âmbito do Open Banking, podendo estes serem dados de diversas categorias, incluindo dados pessoais e dados pessoais sensíveis.[44]

As intersecções entre a Lei Geral de Proteção de Dados e o Open Banking

Respeitar os direitos de privacidade e proteção de dados dos indivíduos é essencial para as instituições financeiras estarem alinhadas às leis e regulações bancárias. As regras e princípios dispostos na LGPD são destinados a facilitar o livre movimento das informações no mercado financeiro, prezando pela proteção dos direitos e interesses das pessoas[45].

Como já abordado anteriormente, o Open Banking se trata de um sistema financeiro aberto, cujo principal objetivo é compartilhar dados e serviços por meio da integração dos sistemas das instituições financeiras.[46] Sendo assim, considerando que a maioria das movimentações financeiras envolvem dados pessoais, é de extrema importância que a legislação e regulações relacionadas ao Open Banking no Brasil estejam em harmonia com a LGPD, principalmente no que se refere aos seus princípios, hipóteses de tratamento e direitos dos titulares de dados pessoais. A importância de funcionar em consonância com a LGPD, além de ser obrigatória sob o ponto de vista hierárquico-normativo, advém da necessidade de conceber que os dados pessoais financeiros tratados pelas instituições financeiras, e consequentemente no ambiente do Open Banking, pertencem aos cidadãos, na maioria das vezes consumidores, que possuem o direito de ter controle a respeito dos seus dados.

A proteção de dados pessoais dos indivíduos deve ser prioridade no âmbito do Open Banking, pois, na maioria das vezes, avisos de privacidade e termos de uso (rara-

mente lidos) não conseguirão controlar e garantir a legitimidade do tratamento de dados pessoais dos indivíduos.[47] Como consequência disso, o consentimento é outro fator facilmente prejudicado, uma vez que muitas vezes ele é fornecido sem a compreensão de seus efeitos.

O compartilhamento de dados pessoais, principalmente os financeiros, pode trazer muitas consequências positivas, como produtos convenientes e personalizados, e maior concorrência entre as diversas instituições financeiras, entretanto isso pode trazer um custo maior em relação à privacidade dos dados, assim como ao controle do uso dos dados pessoais pelos titulares.

Um conceito muito relevante que consta no artigo 2º da LGPD e que deve pautar o tratmento de dados pessoais no âmbito do Open Banking é a autodeterminação informativa, compreendida como um direito não apenas privado, mas coletivo, pois pode afetar muitas vezes direitos difusos.[48] A **autodeterminação informativa** se trata de um direito que cabe a cada pessoa de controlar e de proteger seus dados pessoais, considerando os tempos atuais e a forma que as informações são processadas.[49]

O consentimento está diretamente ligado à autodeterminação informativa, pois por meio dele um indivíduo pode exercer o direito de controlar suas informações pessoais, assim como de protegê-las. O consentimento é uma das chaves para mitigar riscos à privacidade dos dados de titulares no Open Banking, portanto, é necessário que seja criada uma consciência no mercado financeiro de que os dados pessoais tratados e compartilhados por meio da integração de interfaces entre instituições financeiras não as pertencem, e seu uso deve estar sob o controle dos indivíduos, os quais são titulares destes dados.

A Resolução Conjunta nº 4.658/2018 do BCB qualifica o consentimento, estabelecendo, além dos requisitos apontados pela LGPD, que o consentimento deve:

I ser solicitado por meio de linguagem clara, objetiva e adequada;

II ter prazo de validade compatível com as finalidades determinadas, limitado a doze meses;

III discriminar a instituição transmissora de dados ou detentora de conta, conforme o caso;

IV discriminar os dados ou serviços que serão objeto de compartilhamento.[50]

Ainda, a Resolução Conjunta nº 4.658/2018 do BCB veda a obtenção de consentimento por meio de contratos de adesão, formulários com opção de aceite já preenchida ou de manifestação presumida do titular. Essa vedação já exclui práticas antigas de mercado, principalmente às relacionadas a disposições de contratos de adesão, assim como contratos que já vem com o aceite dos clientes, mesmo que estes não os tenham manifestado, obrigando o cliente a ter que se manifestar pela recusa do tratamento (contratos "*opt-out*").

Além de estabelecer procedimentos que se adequem à coleta do consentimento, é necessário que os controladores de dados assegurem a possibilidade de revogação do consentimento dos titulares a qualquer tempo. Além disso, todos os controladores envolvidos no compartilhamento devem ser informados da revogação do consentimento e interromper o tratamento de dados pessoais do titular que realizou a solicitação.

Considerando isso, tanto o BCB quanto a ANPD terão um papel fundamental na fiscalização da gestão do consentimento pelas instituições que integrem o Open Banking, bem como da transparência junto aos titulares, devendo garantir que as instituições obtenham o consentimento do titular, pautadas na LGPD e demais regulações complementares. Dessa maneira, é necessário que leis e regulações conversem entre si, para evitar equívocos normativos e, principalmente, aberturas para que instituições mal-intencionadas procurem lacunas em leis ou regulamentos para tratar dados pessoais em desconformidade ao racional originário da LGPD.

A aplicabilidade dos princípios da qualidade dos dados, transparência e não discriminação da LGPD

A LGPD, em seu artigo 6º, associa seus objetivos e linhas de performance principais em torno de princípios comuns, presentes em vários ordenamentos.[51] No referido artigo, a Lei estabelece 10 alicerces pelos quais suas disposições da LGPD irão se guiar, apontando que o tratamento de dados pessoais deve se pautar pela boa-fé e pelos princípios: da finalidade, da adequação, da necessidade, do livre acesso, da qualidade de dados, da transparência, da segurança, da prevenção, da não discriminação e da responsabilização e prestação de contas.[52]

Como exemplo, a LGPD traz disposições que embasam a necessidade de o tratamento de dados ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular (princípio da necessidade), devendo o referido tratamento ser realizado de forma compatível (princípio da adequação) com a finalidade informada ao titular (princípio da transparência). Ainda, em toda operação de tratamento deve ser garantida a exatidão, clareza, relevância e atualização dos dados (princípio da qualidade de dados), tudo com a observância de o tratamento de dados não ser realizado para fins discriminatórios ilícitos ou abusivos (princípio da não discriminação).

Especificamente, considerando o assunto tratado neste Relatório, assim como a Resolução Conjunta nº 4.658/2018 do BCB, iremos nos ater aos princípios da qualidade dos dados, transparência e não discriminação, também citados na Resolução, em seu artigo 4, incisos I, III e IV.

O **princípio da transparência** está intimamente ligado à relação junto aos clientes das instituições financeiras, pois se trata de uma garantia aos titulares de serem dadas não apenas informações claras e precisas, mas específicas e verídicas. Ainda, mesmo resguardando o segredo comercial e industrial, estes não devem se sobrepor aos direitos do titular e aos outros fundamentos e princípios da LGPD. A transparência junto aos titulares será um dos pontos principais a serem observados para o correto funcionamento do Open Banking, se tornando, a princípio, um desafio, pois envolve diretamente a efetiva gestão do consentimento dos titulares e a necessidade de mapear de forma

otimizada as atividades de tratamento de dados, com o fim de garantir aos titulares informações claras e precisas quanto ao fluxo de tratamento de seus dados pessoais.

A qualidade dos dados também se trata de outro aspecto que deverá ser observado com muita cautela no âmbito do Open Banking, principalmente em relação aos tópicos relacionados à relevância e à minimização dos dados. Isso demandará dos controladores de dados a criação de rigorosos procedimentos "de verificação contínua quanto à exatidão, à clareza, à relevância e à atualização dos dados do titular. O objetivo é manter-se fiel à finalidade de tratamento informada"[53] ao titular, assim como evitar alimentar algoritmos que tomem decisões automatizadas com dados inexatos, desatualizados e sem relevância.

O cuidado com a qualidade dos dados está fielmente ligado ao **princípio da não-discriminação**, considerando que a baixa qualidade dos dados pode afetar não somente a igualdade entre os indivíduos, mas outros direitos fundamentais resguardados não só pela LGPD, mas também pela Constituição Federal. Apesar disso, o mais óbvio e mais estudado impacto relacionado a direitos afetados pela baixa qualidade dos dados é o da não discriminação. Vários estudos e relatórios abordam acerca do uso de dados não representativos ou de algoritmos enviesados que tratam de forma desigual pessoas, baseadas em sua cor, etnia, sexo, orientação sexual, religião, etc. Assim, caso não sejam criadas medidas estruturais que prezem pela qualidade dos dados, nem sejam verificadas a necessidade e a adequação do tratamento, os resultados de decisões automatizadas podem discriminar pessoas baseadas em seus dados sensíveis.[54]

Sob o ponto de vista do Open Banking, dados relacionados à cor, sexo e origem podem afetar ainda mais decisões relacionadas à oferta de crédito de instituições financeiras. Notícias já foram publicadas acerca de descobertas de reproduções de machismo e racismo por algoritmos, principalmente no mercado bancário.[55] Com a integração de todos os dados das instituições financeiras, o direito relativo à não-discriminação pode ser ainda mais afetado, maximizando vieses sistêmicos.

Considerando isso, mais do que olhar apenas para os dados pessoais em si, os órgãos reguladores deverão desenvolver métodos que criem a consciência, tanto pública quanto privada, acerca de como os algoritmos ligados ao sistema aberto do Open Banking irá funcionar, fazendo, assim, com que a base dos algoritmos - os dados - sejam tratados de forma restrita aos fundamentos, princípios e limites da legislação e das regulações. Mais uma vez, a fiscalização das autoridades públicas será fundamental.

Quais os desafios de implementação do Open Banking frente à LGPD e regulações do BCB?

Analisa-se, neste tópico, os desafios para implementação do Open Banking no Brasil a partir da intersecção do que dispõem a Resolução nº 1 de 4 de março de 2020 do BCB, a Lei General de Proteção de Dados Pessoais (LGPD) e outras regulamentações atinentes ao setor financeiro.

É importante salientar que os desafios identificados por este relatório não buscam esgotar as possibilidades do tema, mas tão somente lançar luz sobre possíveis impasses na implementação do Open Banking frente a proteção de dados pessoais.

Os limites para o consentimento

De acordo com a Resolução, as instituições receptoras dos dados[56] ou iniciadora da transação de pagamento[57] deverão, de forma prévia ao compartilhamento dos dados, obter o consentimento do titular[58]. Portanto, depreende-se que a base legal segundo a qual as instituições participantes do Open Banking poderão tratar dos dados referentes (I) ao cadastro do titular e de seus representantes; (II) às transações; e (III) ao encaminhamento de proposta de operação de crédito será o consentimento, disposto nos incisos I, do art. 11[59], ou I, do art. 7º[60], da LGPD, a depender se são dados sensíveis ou não, respectivamente.

Observa-se, a partir de uma análise detida do conceito de consentimento inserido na Resolução, bem como de seus requerimentos dispostos na seção II do capítulo IV, que houve uma preocupação por parte da Diretoria Colegiada do BCB de alinhar os requisitos para o tratamento de dados para fins de implementação do Open Banking àqueles inseridos na LGPD.

Não obstante a importância conferida ao consentimento para a garantia da autodeterminação informativa[61] a partir da 2ª geração de leis de proteção de dados pessoais[62], alguns autores apontam para os limites desta base legal.[63] Problemas relacionados à complexidade do fluxo informacional[64] e as limitações cognoscíveis dos seres humanos no processo de tomada de decisão são os principais fatores que levam a críticas à centralidade do consentimento nas legislações de proteção dos dados pessoais.

No contexto do Sistema Financeiro Aberto, as críticas ao consentimento ganham particular relevância.

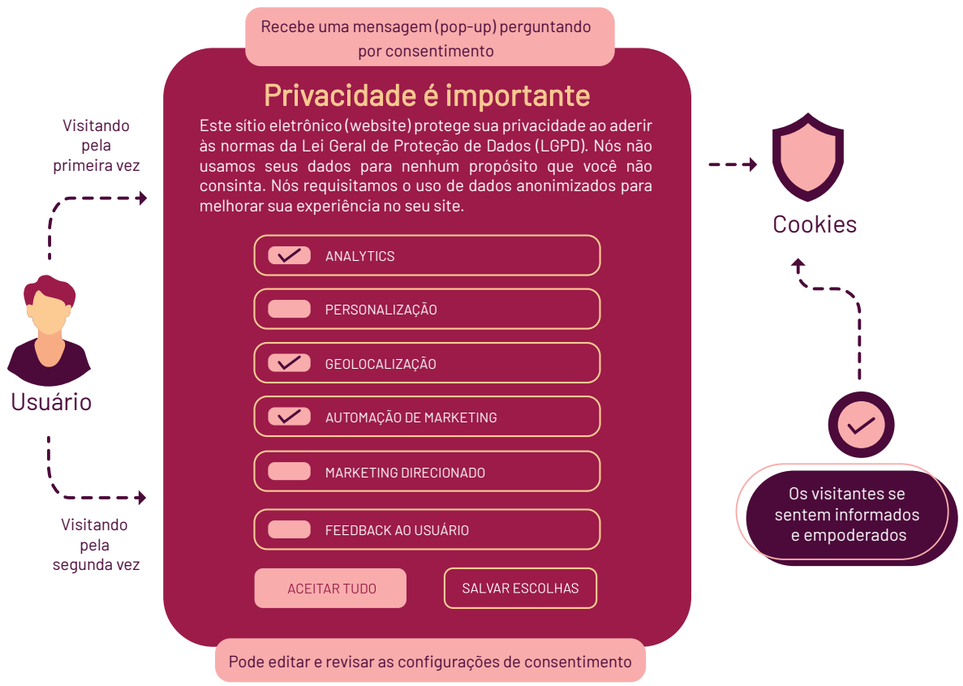
O § 1º do art. 10 da Resolução traz uma série de requerimentos para que as instituições, que são receptoras de dados e iniciadoras de transação de pagamento, obtenham o consentimento dos clientes. Dentre os requisitos, destacam-se a necessidade da solicitação (I) ser obtida por meio de linguagem clara, objetiva e adequada, (II) referir-se a finalidades determinadas (III) discriminar a instituição transmissora de dados ou detentora de conta, conforme o caso e (IV) discriminar os dados ou serviços que serão objeto de compartilhamento. Ademais, quando ocorram alterações das condições de que tratam os incisos II a V, a Resolução impõe a necessidade da obtenção de um novo consentimento do titular.

Os amplos requisitos dispostos no art. 10 da Resolução podem levar à **fadiga do consentimento**[65], situação na qual o titular se vê frente a inúmeras solicitações, resultando em um extenso conteúdo e complexidade na avaliação das consequências da autorização para o tratamento de seus dados pessoais. Aliás, não será apenas o consentimento para os dados tratados no âmbito do Sistema Financeiro Aberto que o titular irá se deparar. Pelo contrário, Aleecia e Lorrie[66], em 2008, já alertavam para o fato de ao cidadão norte americano ser apresentado em média 1,462 políticas de privacidade por ano, representando uma estimativa de 244 horas e um valor de aproximadamente 3,534 dólares americanos por ano. Nesse contexto, Daniel Solove[67], partindo da análise de pesquisas quantitativas sobre os limites do consentimento, expõem que os titulares tendem a não ler as políticas de privacidade ou os alertas para consentimento, seja por não entenderem o conteúdo transmitido seja por fazerem inferências errôneas acerca

de como os dados serão tratados.

Adverte-se, no entanto, que as críticas aqui tecidas não têm como objetivo a desconsideração do consentimento como base legal para o tratamento dos dados referentes ao Open Banking. Pelo contrário, é justamente por compreender a importância de que o titular assuma o protagonismo do seu direito à autodeterminação informativa que situamos o consentimento como desafio de implementação do Open Banking frente à LGPD.

Nesse cenário, por exemplo, o *European Data Protection Board* (EDPB)[68], em 04 de maio de 2020, ao elaborar diretrizes para o consentimento diante do Regulamento Geral de Proteção de Dados Pessoais (RGPD ou GDPR), traça importantes considerações sobre como fornecer um consentimento informado, adjetivo também presente na resolução do BCB[69]. Segundo o EDPB, para a obtenção de um consentimento válido, dentre outros requisitos, o controlador precisa garantir uma linguagem clara e objetiva, de forma que seja facilmente compreendida pela figura do "pessoal média". Daniel Solove[70], também debruçando-se sobre possíveis soluções, propõem uma abordagem para a obtenção do consentimento que leve em consideração as descobertas das ciências sociais sobre como os titulares tomam decisões acerca de seus dados pessoais e os limites cognitivos de tais decisões.



O Conselho Diretor do BCB parece reconhecer os desafios que a utilização desta base legal ensejará. A Resolução, com o fito de promover objetividade no processo de obtenção do consentimento, possibilitou a apresentação dos dados referentes ao compartilhamento de forma agrupada, desde que obedecidos determinados critérios.[71]

Por fim, mas não menos importante, os desafios impostos pelo consentimento diante da implementação do Sistema Financeiro Aberto somente poderão ser devidamente enfrentados por meio do comprometimento assíduo dos controladores na observância dos direitos dos titulares e, sobretudo, dos princípios da finalidade[72], da adequação[73], da necessidade[74], da transparência[75], da segurança[76] e da não discriminação[77].

Segurança Cibernética

O aumento do fluxo de dados proporcionado pelo Open Banking também gera desafios no que se refere à segurança cibernética. A Resolução, na seção V do capítulo V, dispõe sobre "mecanismos de acompanhamento e controle com vistas a assegurar a confiabilidade, a disponibilidade, a integridade, a segurança e o sigilo"[78] em relação ao compartilhamento de dados e serviços advindos do Open Banking.

Os dados abrangidos pelo compartilhamento no Sistema Financeiro Aberto são de significativa importância para a vida pessoal dos titulares, uma vez que podem identificar quanto uma pessoa ganha, com o que o dinheiro é gasto, com que medida é gasto a mais do que se ganha, se o titular é membro de algum partido político ou religião, o quão frequente o titular vai ao médico ou faz atividades físicas, entre outros aspectos. Estes exemplos ajudam a ilustrar que alguns dos dados compartilhados possuem natureza sensível, o que implica na necessidade de proteção especial, conforme regula a LGPD.

Dado o alto grau de sensibilidade dos dados financeiros, a segurança cibernética ganha especial relevância no âmbito do sistema financeiro. Afinal, este setor é alvo frequente dos ataques cibernéticos, também conhecidos como cibercrimes. De acordo com pesquisa da NetDiligence[79], durante o período entre 2014 e 2018 as reclamações de segurança cibernética no setor financeiro ocupou o terceiro lugar em número de ataques.

Nesse contexto, tanto as instituições de pagamento como as instituições financeiras já estavam submetidas a regulamentação do Banco Central do Brasil quanto aos aspectos relacionados a políticas de segurança cibernética, de acordo com a Circular nº 3.909/2018 e com a Resolução nº 4.658/2018, respectivamente.

No entanto, as regulamentações supracitadas estabelecem que as políticas de segurança deverão ser compatíveis, dentre outros fatores, com o porte das instituições [80]. Sabe-se, nesse sentido, que um dos objetivos centrais do Open Banking é possibilitar a competitividade no setor por meio da facilitação de entrada de novos atores[81]. Um dos exemplos são as startups que carecem de estrutura financeira que possibilite a devida segurança, integridade e sigilo dos dados.

No enfrentamento do desafio aqui exposto, o BCB, ao definir o conteúdo mínimo das políticas de segurança cibernética, estabelece que as intuições deverão adotar procedimentos e controles no intuito de reduzir vulnerabilidades a incidentes e, inclusive, deverão adotar tais medidas quando do desenvolvimento de sistemas de informação[82].

Esta obrigação imposta de *Security by Design*[83] encontra ressonância no §2º, do art. 46 da LGPD, que dispõe que a obrigatoriedade de medidas técnicas e administrativas aptas a proteger os dados pessoais de acesso não autorizado deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução[84].

O Open Banking e a cooperação entre Autoridades

O Grupo de Pesquisa da Universidade Livre de Bruxelas, *Data Protection on the Ground*, em uma mesa redonda com diversos atores ligados aos sistemas financeiro europeu para discutir os desafios da implementação da Diretiva PSD2, assinalou que "diferentes regulamentações que afetam o setor financeiro podem entrar em conflito"[85]. Segundo o grupo, ao passo que as autoridades de proteção de dados requerem aos bancos um restrito compartilhamento de dados, as autoridades antitruste, por sua vez, requerem o oposto[86]. Nesse cenário, a orientação do grupo é que exista colaboração entre as autoridades supervisoras e sejam desenvolvidas diretrizes conjuntas para o setor financeiro[87].

Tais inquietações apresentadas no âmbito da Diretiva Europeia podem ser transpostas ao contexto brasileiro referente ao Sistema Financeiro Aberto, resguardada as particularidades de cada caso.

Nesse contexto, o desafio deste tópico refere-se à necessidade de uma atuação conjunta, não só entre a ANPD, Conselho Administrativo de Defesa Econômica (CADE) e BCB, como de todas as autoridades ligadas ao setor, como por exemplo a Secretaria Nacional do Consumidor (Senacon).

De início, cabe ressaltar que, infelizmente, a Resolução que dispõe sobre o Open Banking não contou com uma avaliação da ANPD no que se refere à proteção de dados pessoais, já que a autoridade, apesar de vigente segundo a Lei, ainda não foi constituída pelo Governo Federal.

Segundo o inciso XXIII do art. 55-J da LGPD, compete à ANPD articular-se com as autoridades regulatórias públicas para exercer suas competências em setores específicos de atividade econômicas e governamentais sujeitas a regulamentação[88]. Ademais, o §3º do mesmo artigo dispõe que a ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados, conforme legislação específica, e o tratamento de dados pessoais, na forma desta Lei.

A título de exemplo, os desafios expostos no tópico 4.2 e 4.3 poderiam ganhar um elemento de previsibilidade por meio de um trabalho conjunto entre o BCB e a ANPD. No que se refere ao consentimento e as interfaces dedicadas ao compartilhamento de dados do Open Banking, a ANPD poderia atuar de forma a estimular a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais[89].

Já as preocupações com a segurança cibernética advindas da entrada de startups e microempresas no fluxo dos dados proporcionados pelo Open Banking poderiam ser amenizadas caso a ANPD, segundo sua competência prevista no inciso XVIII do art. 55-J, editasse normas, orientações, e procedimentos simplificados para microempresas e empresas de pequeno porte, bem como aquelas que se autodeclarem startups ou empresas de inovação.

Quais as eficiências e os entraves econômicos para as empresas que adotarem o Open Banking?

Esta sessão levanta considerações sobre impactos econômicos positivos e possíveis impactos negativos da operacionalização do Open Banking no mercado brasileiro. Ainda, apresentamos também alguns questionamentos e soluções privadas e de políticas públicas para lidar com as adversidades dessa mudança de paradigma econômico em direção à uma modernização do mercado brasileiro.

O posicionamento do sistema bancário brasileiro

O Banco Central do Brasil, através da sua Agenda BC#, já sinalizou que o país está a caminho de uma profunda reforma no setor bancário, orientada pela regulamentação do Open Banking. Essa formatação leva a profundas mudanças em diversos setores econômicos, mais especificamente no comércio eletrônico (*e-commerce*) e nas finanças de pessoas e empresas, especialmente nas relações entre clientes, bancos e micro-empresários. Dessa forma, destacam-se potenciais ganhos, preocupações e possíveis soluções para que a transição explore bem as potencialidades positivas dessa tendência nos mercados mundiais.

O Open Banking é especialmente explorado pelas Pequenas e Médias Empresas (PMEs), por compreenderem suas alternativas para melhor gerirem suas decisões financeiras e novas possibilidades de mercados e parcerias. Por ser um modelo de compartilhamento padronizado de dados e serviços bancários, aliados a diversas plataformas e fontes de dados, existem várias implicações no que diz respeito aos novos gargalos de custos e oportunidades, a partir de um fluxo mais dinâmico de renda e informação. Os benefícios potenciais do Open Banking, que serão explorados mais adiante, são substanciais: melhoria da experiência do cliente, novos fluxos de receita, menores custos de transação, quebra da assimetria e monopólio de informação e maior capacidade de absorver mercados tradicionalmente mal atendidos.

A transição, no entanto, não é tão direta com uma tendência evolucionária de pagamentos. Ainda que nos anos recentes tenha surgido diversos "ecossistemas digitais de pagamentos", como os chineses Tencent (WeChat) e Alibaba (AliPay), exemplos de sistemas maduros e massivos que colidem entre si, fazem com que a proposta de compartilhamento de dados financeiros seja um conflito de interesses entre setores que já se estabeleceram e se aproveitam da posição de monopólio, frente à abertura do Open Banking[90].

O setor bancário, por exemplo, ainda observa o Open Banking mais como uma ameaça do que uma oportunidade. Contudo, é necessário se fazer uma contextualização do setor bancário brasileiro para melhor entender esse cenário. Com base nas pesquisas de acesso[91] e desenvolvimento[92] bancário-financeiro do FMI, podemos trazer uma luz maior ao debate das possibilidades de ganho e perdas do setor bancário brasileiro.

O setor bancário brasileiro é bem desenvolvido. Em relação ao índice de Desenvolvimento Financeiro do FMI, que é um ranking relativo de países na **profundidade, acesso, eficiência de suas instituições e mercado financeiro, o Brasil se posiciona na 20º posição**, de 136 países contabilizados. No entanto, devemos fazer algumas considerações sobre como esse índice é construído e quais as vantagens e desvantagens do setor bancário brasileiro, que poderiam ser exploradas pelo Open Banking.

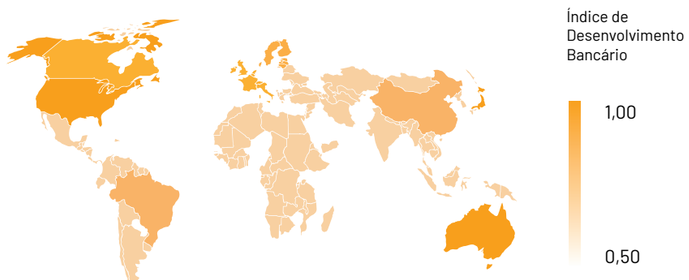
Em primeiro lugar, quando analisamos o índice de acesso bancário (que varia de zero a um), considerada a distribuição geográfica e a quantidade de filiais bancárias e caixas eletrônicos, o Brasil aparece na 19ª posição. Sua pontuação é maior do que todos os países da América Latina, África e Leste Asiático (à exceção da Tailândia e Japão).

No entanto, as instituições bancárias brasileiras, especialmente quando comparamos com o mercado financeiro nacional, são pouco eficientes e caras. Inicialmente,

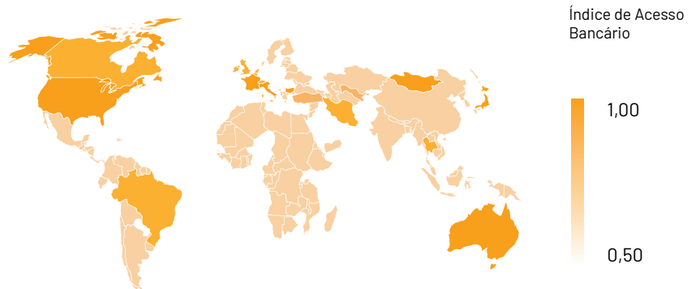
o índice de eficiência do mercado financeiro, que contabiliza a taxa de retorno nos mercados de capital brasileiro, coloca o Brasil na 8ª posição do ranking. Quando levantamos os dados do setor bancário, no que diz respeito à margem financeira líquida do setor bancário, spread de depósitos e empréstimos, receita sobre juros sobre receita total, custos indiretos sobre ativos totais, retorno sobre ativos e retorno sobre patrimônio. **Sobre a eficiência do setor bancário brasileiro, o Brasil cai para a 109ª posição do ranking, refletindo a defasagem estrutural dos bancos nacionais**.

As pontuações dos países pelos índices podem ser visualizadas em um mapa de gradiente de cores nas imagens a seguir, em que cores mais escuras representam uma maior pontuação[93]:

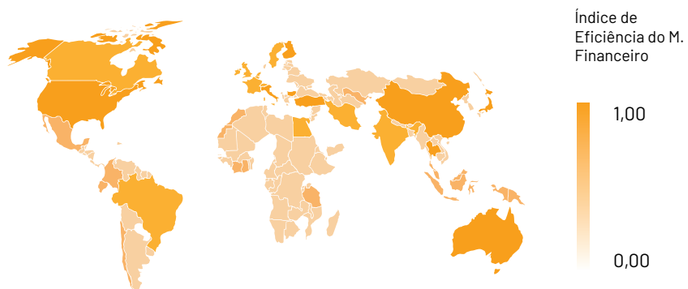
1 Mapa-mundi do Índice de Desenvolvimento Bancário



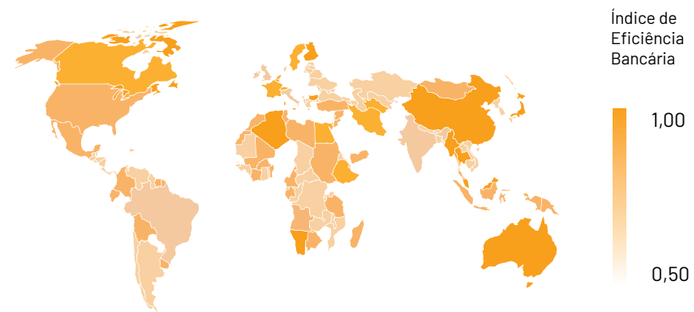
2 Mapa-mundi do Índice de Acesso Bancário



3 Mapa-mundi do Índice de Eficiência do Mercado Financeiro



4 Mapa-mundi do Índice de Eficiência Bancária



Portanto, **o desenvolvimento do setor financeiro brasileiro foi baseado na sua distribuição física e desenvolvimento eficiente do mercado financeiro**. Enquanto isso, com base em uma estrutura oligopolizada e com barreiras de entrada pouco eficiências, desenvolvemos um **sistema bancário caro, pouco produtivo e burocrático**. Isso se reflete também em alguns comportamentos da população brasileira. Por exemplo, no Brasil a taxa de poupança é menor do que a do Chile, Uruguai, Colômbia, Bolívia, África do Sul, Turquia, Rússia, colocando em 77º em uma lista de 108 países.

A desconfiança do setor bancário tradicional ao Open Banking

Existem **duas razões diretas** para esse tipo de comportamento. Em primeiro lugar, os bancos são hoje diretamente beneficiados pelo monopólio de dados bancários de seus correntistas; em segundo lugar, serão os insurgentes não-bancários os que demonstraram a maior tração de mercado e com maior potencial de ganho de novos clientes[94].

A forma atual de atuação dos bancos garante uma certa tutoria sobre os dados e informações financeiras de seus clientes. É construída uma relação paternalista de confiança entre banco e cliente que possui dois aspectos, um positivo e um negativo. O aspecto positivo é a segurança dos dados dos correntistas, podendo ser pessoa física ou jurídica. Não somente pelo firmamento do contrato garantindo o direito à privacidade financeira, é interesse direto dos bancos manter total segredo dos dados sob sua tutela, uma vez que existe uma oportunidade econômica direta desse tipo de ativo.

Essa oportunidade econômica, em um sistema com pouca competição, leva ao aspecto negativo da relação de confiança. Os bancos utilizam essa exclusividade das informações de seus clientes para vender produtos e serviços caros, pouco eficientes e com baixo valor agregado. Valendo-se de um custo de transação maior, muitas vezes não compensa ao correntista extrair seu dinheiro ou informação financeira para outras plataformas mais eficientes, restringindo-se aos ofertados pelo banco de origem. Essa qualidade do sistema bancário brasileiro auxilia a manutenção de serviços pouco eficientes e de baixo valor agregado, refletindo na posição brasileira no ranking de eficiência bancária.

As oportunidades do Open Banking ao setor bancário

Apesar de ser inevitável afirmar que o Open Banking vai resultar em algum grau de sacrifício ao setor bancário em seu controle econômico, **os bancos poderão se beneficiar da participação em um maior "*profit pool*" em todos os setores economicamente impactados**. Os bancos, especialmente os brasileiros, podem aproveitar sua posição de liderança para criar serviços direcionados ao Open Banking, sejam estes serviços de previsão analítica, inteligência artificial, ou ainda, financiamento de consumidores e PMEs.

Também é esperado que os bancos se tornem mais experientes na forma como eles obtêm e analisam dados de seus correntistas. Não somente dados bancários, mas todo tipo de atividades e interações, para obter melhor conhecimento sobre seus clientes. A realidade, para o setor bancário, é que a habilidade dos bancos de satisfazerem um maior número de necessidade de seus clientes é intrínseca para seu faturamento. O Open Banking tem o potencial de auxiliar os bancos a conhecerem seus correntistas, seus padrões de comportamento, financeiro, investimento, de saúde e objetivos[95] e encontrarem novos nichos de atuação. O Open Banking, inclusive, devido à abertura de dados, cria uma demanda por aplicativos de pagamentos centrais rápidos e eficientes, o que é expertise de alguns bancos.

Brodsky e Oakes[96] elencam algumas estratégias a serem adotadas por bancos para capitalizar as vantagens oriundas do Open Banking:

I Explorar acordos de compartilhamento de dados com *fintechs* e empresas não financeiras de serviço para antecipar a legislação;

II Desenvolver uma perspectiva sobre APIs e seus benefícios ao modelo de serviço bancário, potencialmente expandindo o acesso de terceiros para além dos requerimentos legais;

III Compreender a legislação de privacidade de dados vigente e possíveis mudanças e;

IV Analisar o apetite da instituição para abordagens menos ortodoxas de serviço e examinar a reação dos clientes, de forma a facilitar tal mudança.

Os benefícios gerais do Open Banking estão relacionados aos ganhos de eficiência oriundo da quebra das ilhas e assimetrias de informação. Alguns **impactos positivos por grupos econômicos** são elencados a seguir, de acordo com Hallsworth *et al*[97]:

- **Fornecedores *front-end***: esses agentes se concentrarão em oferecer uma experiência superior ao consumidor e acesso a uma variedade de produtos e serviços de bancos e terceiros, por meio de agregação e segmentação de produtos. Eles serão os "orquestradores do ecossistema", entregue por meio das APIs, incorporados à vida dos clientes.
- **Especialistas de produtos**: grupo que se concentra em tornar cada vez mais ágil o desenho e aprimoramento de produtos para seus clientes. O design do produto será complementado por todo o mapeamento de informações e captação de algoritmos da plataforma *front-end*, que funciona para garantir que os produtos continuem altamente recomendados.
- **Gigantes da infraestrutura**: se beneficiarão das economias de escala e eficiência operacional, cooptando participantes para se tornarem fornece dores de sua estrutura de *back-end* para o setor bancário (que fornece essencialmente a infraestrutura de pagamentos que mantêm o sistema em operação).

O Open Banking também oferece algum impacto em termos econômicos bem expressivos, que auxiliam na eficiência do mercado, como um todo, como por exemplo, na questão da quebra da assimetria de informação. Atualmente possuímos ilhas informacionais a respeito tanto das movimentações financeiras dos consumidores, quanto de seu perfil de consumo ou inclinações pessoais obtidas de plataformas sociais. O Open Banking gera uma quebra da assimetria de informação, ao centralizar diferentes tipos de informação, que atua diretamente na incerteza dos fornecedores e compradores no momento da realização de um contrato ou no design de um produto ou serviço. O escopo de **informações centralizadas e de "fácil acesso"**, ajuda a reduzir, por exemplo, o risco associado de uma negociação, por trazer um perfil mais completo dos indivíduos, fazendo com que se aumente a agilidade e se reduzam os processos, os riscos e os custos associados.

Essa característica também ajuda a personalizar acertos financeiros, a depender do perfil financeiro e de compra dos clientes, no sentido de dar mais sustentabilidade a negociação de crédito, dívidas, formas de pagamento, a depender dos critérios de avaliação da parte fornecedora[98/99].

Ademais, o Open Banking permite a potencialidade de **parcerias mais amplas**, gerando a oportunidade de se criar combinações de produtos e serviços sem o custo e o inconveniente de se negociar com múltiplas companhias[100].

Para o caso de PMEs, o desenvolvimento de novos sistemas de pagamentos, tutorados pela LGPD e pela legislação de Open Banking, desenvolvem novos nichos de dados? que capacitam as PMEs a reconciliarem instantaneamente suas finanças, sem a necessidade de tratamento manual, reduzindo custos de contabilidade e facilitando, por exemplo, o pagamento de impostos.

Riscos do Open Banking ao sistema financeiro

Ao passo de criar certos benefícios, o desenvolvimento do Open Banking também pode criar perigos potenciais. As ferramentas mencionadas anteriormente podem gerar ou potencializar **conflitos de interesse, exploração de assimetrias de poder e exacerbar a exclusão financeira**. Conveniência, simplicidade e velocidade podem vir às custas de perda de controle sobre o dinheiro, redução de privacidade ou segurança e maior complexidade dos mercados.

A instrumentalização do uso de comissões em plataformas que desenham modos de venda e produtos, a partir de uma análise do perfil das empresas e consumidores, pode introduzir um **viés de consumo**. Os malefícios do viés do consumo recaem tanto sobre consumidores, quando sobre vendedores.

O efeito nocivo sobre o cliente é que, da mesma forma que diversos produtos que lhe são apresentados não o seriam sem o aperfeiçoamento da leitura de dados, acaba limitando sua liberdade de escolha entre uma infinidade de produtos, a depender dos estímulos de comissão de cada plataforma a comercializar um tipo de produto em detrimento de outro.

Pelo lado das empresas, se não há uma grande competição entre APIs, o modelo de mercado competitivo não é posto em prática, excluindo produtos e serviços que pagam comissões menores, ou que não possuem acesso direto às plataformas, especialmente os pequenos comércios locais.

Existem três possíveis maneiras de se corrigir estes problemas: 1) estimular competição entre APIs, reduzindo as assimetrias entre comissões; 2) conduzir pequenos comércios e empreendimentos locais para o sistema de vendas e finanças online e; 3) introduzir um sistema de comissões fixas por tipo de produto, de modo que as plataformas não tenham um estímulo econômico para introduzir um viés de escolha no consumidor.

Ainda, quando tratamos de conexão de diversos empreendimentos em plataformas centralizadas, nos deparamos com um outro problema econômico, denominado **assimetria de poder**. Essa assimetria surge quando um agente possui mais informação e/ou recursos do que o outro (como consumidores ou PMEs). Tradicionalmente[101], em relação às finanças, a assimetria de poder beneficiou grandes empresa e bancos. O desenho de produtos muitas vezes é complexo e a fixação de termos e condições geralmente são longas e difíceis de se compreender, notadamente excludentes.

Atualmente é difícil para grande parte dos consumidores e PMEs a compreensão de quais dados diários são produzidos por eles e como isso beneficia terceiros. Dessa forma, o compartilhamento de dados possibilita serviços e produtos convenientes e personalizados, mas pode permitir um descontrole e falta de transparência em relação às cadeias de provedores e compartilhamento de dados. Quando não há uma legislação sobre proteção de dados, surge a possibilidade, portanto, de diversas empresas oferecerem serviços "gratuitos", quando estão ao mesmo tempo monetizando acesso aos dados dos clientes, concedidos por consentimento duvidoso ou não muito claro, por parte do consumidor.

Como afirmado, sob a atual jurisdição, é papel dos bancos assegurar a proteção os dados financeiros e transacionais de seus clientes, sejam eles pessoas físicas ou jurídicas. Com a introdução do Open Banking, a "custódia" dos dados financeiros pelos bancos seria rompida trazendo o risco de que dados financeiros estariam, juntamente com diversos dados já coletados por diferentes plataformas, à disposição de interesses econômicos pouco claros.

Por último, um potencial problema que pode ser exacerbado por meio do Open Banking é a exclusão financeira e digital. O Brasil apresenta um baixo nível de transações financeiras feitas por meios móveis, o que é um indicativo de alto nível de exclusão digital. O volume de transações em relação do PIB dos países, no Brasil, é quase a metade dos observados na Rússia, Costa Rica e Chile, por exemplo. De acordo com dados do FMI[102], o volume transacionado no Brasil possui paralelos na Bulgária, Sérvia e Vietnã. Esse dado não reflete necessariamente a falta de acesso a smartphones ou Internet, como também reflete falta de confiança nesses meios para algum tipo de transação bancária, o que pode ser consequência do bom índice de acesso bancário brasileiro ou preferência (por questões culturais ou de baixo aprendizado em mídias digitais) pelo contato físico com a estrutura bancária em detrimento do digital.

A natureza destes tipos de exclusão, no entanto, será exacerbada pelo potencial aumento dos benefícios que consumidores e empresas terão acesso. Os maiores beneficiados serão os agentes que já possuem algum tipo de familiaridade ou predominância nas plataformas de comércio e finanças digitais. Por esse lado, defende-se a necessidade de se promoverem políticas públicas de educação em finanças e gestão de dados. A educação financeira é pilar para que os consumidores e PMEs consigam usufruir dos benefícios oriundos da potencialidade do Open Banking compreendendo, sempre os gargalos naturais para esses tipos de tecnologia.

Sobre a exclusão puramente financeira, grupos já marginalizados poderiam aprofundar esse "*gap*" de renda. Algumas informações, como gênero, identidade e endereço podem incluir mais uma barreira para acesso de alguns tipos de serviços e produtos. Existem produtos que lideraram entusiasmos para a resolução das desigualdades do gênero financeiro, como *ipagoo*, um serviço de pagamentos europeu que auxilia jovens, idosos e usuários de baixa renda a priorizarem e organizarem suas contas. No entanto, ainda há ceticismo sobre a representatividade dos ganhos em populações de baixa renda, uma vez que o mercado tende a atender o maior potencial de renda e excluir os outros.

Conclusão

Destarte, a essencialidade de uma lei que garanta direitos e deveres no que tange à propriedade e compartilhamento de dados é clara. Dessa forma, defende-se que a Lei Geral de Proteção de Dados seja aplicada desde a concepção do ambiente de Open Banking brasileiro, garantindo ao consumidor e PMEs, maior segurança na sua geração e compartilhamento de informações, nas quais serão incluídos, com o Open Banking também dados financeiros. Dessa forma, não só é garantido o direito de proteção dos dados, como o aumento da transparência de uso e aplicação das informações obtidas de cada cliente, reduzindo assimetrias de poder geradas por vieses de informação.

Como citado, o maior acesso a dados financeiros pode gerar uma maior personalização de acesso ao crédito. Não necessariamente relacionado ao crédito bancário, mas ao crédito de consumo direto, ou seja, quando o cliente negocia diretamente com a plataforma de venda os termos de pagamento do produto. Este modelo pode levar a meios mais eficientes e mais baratos de crédito, mas, ao mesmo tempo, a uma prática de crédito mais agressiva e disponibilização irresponsável. Ainda, segundo Reynolds (2017)[103], especialistas em consumo observaram que o acesso aos dados financeiros do cliente ou PMEs dá maior poder ao operador de crédito, especialmente se puder ser observado que o solicitante está em uma situação de restrição ao crédito. Por outro lado, clientes que possuem uma maior capacidade de pagamento podem ser induzidos a uma negociação mais restrita ou descontos menores na aquisição de bens ou serviços.

A hígida aplicação das bases legais ao tratamento de dados pessoais pelas instituições financeiras implicará diretamente na eficiência e qualidade das informações circuladas no mercado financeiro e, consequentemente, no Open Banking. Assim, instituições financeiras e órgãos reguladores deverão trabalhar de forma harmônica e em conjunto acerca do correto uso das hipóteses dispostas na legislação. Para tratar dados sensíveis, o artigo 11º da LGPD delimita que este poderá ocorrer, em regra, apenas com o consentimento específico e destacado do titular, devendo o tratamento ser realizado para finalidades específicas.

Considerando isso, tanto o BCB quanto a ANPD terão um papel fundamental na fiscalização da gestão do consentimento pelas instituições que integrem o Open Banking, bem como da transparência junto aos titulares, devendo garantir que as instituições obtenham o consentimento do titular, pautadas na LGPD e demais regulações complementares.

Dessa maneira, é necessário que leis e regulações conversem entre si, para evitar equívocos normativos e, principalmente, aberturas para que instituições mal-intencionadas procurem lacunas em leis ou regulamentos para tratar dados pessoais em desconformidade ao racional originário da LGPD.

Referências

Introdução

1.
JONES, Rupert. Barclays to sell customer data. The Guardian, 2013, p. 1. Disponível em: https://www.theguardian.com/business/2013/jun/24/barclays-bank-sell-customer-data. Acesso em: 3 mar. 2020.

Introdução ao Open Banking

2.
OPEN BANKING. Background to Open Banking, 2018. Disponível em: <https://www.openbanking.org.uk/wp-content/uploads/What-Is-Open-Banking-Guide.pdf>. Acesso em: 18 set. 2020.

3.
BERLIND, David. APIs Are Like User Interfaces—Just With Different Users in Mind, 2015. Disponível em: <https://www.programmableweb.com/news/apis-are-user-interfaces-just-different-users-mind/analysis/2015/12/03>. Acesso em: 12 set. 2020.

4.
EUROPEAN UNION. Directive (EU) 2015/2366 Of The European Parliament And Of The Council. Official Journal of the European Union, 2015. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX : 32015L2366 & from=PT>. Acesso em: 16 ago. 2020.

5.
ZACHARIADIS, Markos; OZCAN, Pinar. The API Economy and Digital Transformation in Financial Services: The Case of Open Banking (June 15, 2017). SWIFT Institute Working Paper No. 2016-001. Disponível em: <https://ssrn.com/abstract=2975199 or http://dx.doi.org/10.2139/ssrn.2975199>. Acesso em: 17 jul. 2020.

6.
EURO BANKING ASSOCIATION. Open Banking Working Group, 2018. Disponível em: <https://www.abe-eba.eu/thought-leadership-innovation/open-banking-working-group/>. Acesso em: 17 ago. 2020.

A Lei Geral De Proteção De Dados e o Open Banking

7.
ASSEMBLEIA GERAL DA ONU. Resolução 217 A (III). Paris, 10 de dezembro de 1948. Declaração Universal dos Direitos Humanos. Disponível em: <https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=por>. Acesso em: 17 de maio de 2020.

8.
FREUDE, Auvar; FREUDE, Trixy. Echoes of History: understanding german data protection. Understanding German Data Protection. 2016. Disponível em: https://www.bfna.org/research/echos-of-history-understanding-german-data-protection/. Acesso em: 17 de maio de 2020.

9.
FREUDE, Auvar; FREUDE, Trixy. Echoes of History: understanding german data protection. Understanding German Data Protection. 2016. Disponível em: https://www.bfna.org/research/echos-of-history-understanding-german-data-protection/. Acesso em: 17 de maio de 2020.

10.
ÖMAN, Sören. Implementing Data Protection in Law. Dispo- nível em: < http://www.scandinavianlaw.se/pdf/47-18.pdf >. Acesso em: 20 de maio de 2020.

11.
COUNCIL OF EUROPE. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. 10 jan. 1981. Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108> Acesso em 17 de maio de 2020.

12.
COMITÊ GESTOR DA INTERNET Resolução CGI.br/RES/2009/003/. Disponível em: https://www.cgi.br/resolucoes/documento/2009/00. Acesso em 31 de maio de 2020.

13.
C MARA DOS DEPUTADOS. PL 4060/2012. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao? idProposicao=548066. Acesso em 31 de maio de 2020.

14.
BRASIL, Lei Federal 12.965. Marco Civil da Internet. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 7 de maio de 2020.

15.
ESTADÃO. Câmara cria comissão para analisar Lei de Proteção de Dados Pessoais. Disponível em : https://link.estadao.com.br/noticias/cultura-digital,camara-cria-comissao-para-analisar-lei-de-protecao-de-dados-pessoais,10000084559. Acesso em 30 de maio de 2020.

16.
DATA PRIVACY BR, Observatório. 2019. Disponível em: <https://observatorioprivacidade.com.br/memoria/2018-uma-conjuncao-astral/>. Acesso em 20 de maio de 2020.

17.
Idem.

18.
MONTEIRO, Renato Leite et al (org.). Lei Geral de Proteção de Dados e GDPR: histórico, análise e impactos. histórico, análise e impactos. 2018. Página 11. Baptista Luz Advogados. Disponível em: https://www.academia.edu/38940887/Lei_Geral_de_Prote%C3%A7%C3%A3o_de_Dados_e_GDPR_hist%C3%B3rico_an%C3%A1lise_e_impactos. Acesso em: 17 de maio 2020.

19.
BRASIL. Congresso Nacional. Medida Provisória n° 869, de 2018 (Proteção de dados pessoais). Disponível em: https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/135062. Acesso em: 7 de junho de 2020.

20.
BRASIL. Lei 13.853/2019. Altera a Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 7 de junho de 2020.

21.
A OMS declarou pandemia de Covid-19 no dia 11 de março de 2020. Na época a doença já estava presente em 110 países de todos os continentes. Disponível em <https://www.bbc.com/portuguese/geral-51842518>. Acesso em 7 de junho de 2020.

22.
BRASIL. Lei 1179/2020. Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do Coronavírus (Covid-19). https://www25.senado.leg.br/web/atividade/materias/-/materia/141306

23.
BRASIL, Medida Provisória 959/2019. Disponível em: https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/141753. Acesso em: 7 de maio de 2020.

24.
BRASIL, Lei Federal 13.705/2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 16 de maio de 2020.

25.
BRASIL, Constituição Federal (1988). Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 16 de maio de 2020.

26.
Art. 5º da LGPD.

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

27.
BRASIL, Lei Federal 13.705/2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 16 de maio de 2020.

28.
Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:

I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

II - realizado para fins exclusivamente:
a) jornalístico e artísticos; ou
b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;

III - realizado para fins exclusivos de:
a) segurança pública;
b) defesa nacional;
c) segurança do Estado; ou
d) atividades de investigação e repressão de infrações penais; ou

IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

29.
EUROPA. EDPS. Guidelines on data protection in EU financial services regulation. p. 15. Disponível em: https://edps.europa.eu/sites/edp/files/publication/14-11-25_financial_guidelines_en.pdf. Acesso em: 7 de junho de 2020.

30.
Ibidem.

31.
BRASIL, Lei Federal 13.705/2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 16 de maio de 2020.

32.
EUROPA. EDPS. Guidelines on data protection in EU financial services regulation. p. 15. Disponível em: https://edps.europa.eu/sites/edp/files/publication/14-11-25_financial_guidelines_en.pdf. Acesso em:7 de junho de 2020.

33.
BRASIL, Banco Central do Brasil, Resolução nº 4.658 de 26 de Abril de 2018. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. Disponível em: https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50581/Res_4658_v1_O.pdf

34.
BRASIL. Governo Federal. Guia de Boas Práticas para Implementação na Administração Pública Federal. 1 v. 11, 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf. Acesso em: 16 de maio de 2020.

35.
Inciso XII, artigo 5 da LGPD. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 16 de maio de 2020.

36.
Artigo 2º da LGPD.

37.
"Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

§ 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas. § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público. § 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores. § 6º Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor."

38.
Lei 13.709/2018. "Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente."

39.
Lei 105/2001. "Art. 1o As instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados."

40.
"Art. 1. § 3o Não constitui violação do dever de sigilo:

I – a troca de informações entre instituições financeiras, para fins cadastrais, inclusive por intermédio de centrais de risco, observadas as normas baixadas pelo Conselho Monetário Nacional e pelo Banco Central do Brasil;

II - o fornecimento de informações constantes de cadastro de emitentes de cheques sem provisão de fundos e de devedores inadimplentes, a entidades de proteção ao crédito, observadas as normas baixadas pelo Conselho Monetário Nacional e pelo Banco Central do Brasil;

III – o fornecimento das informações de que trata o § 2º do art. 11 da Lei no 9.311, de 24 de outubro de 1996;

IV – a comunicação, às autoridades competentes, da prática de ilícitos penais ou administrativos, abrangendo o fornecimento de informações sobre operações que envolvam recursos provenientes de qualquer prática criminosa;

V – a revelação de informações sigilosas com o consentimento expresso dos interessados;

VI – a prestação de informações nos termos e condições estabelecidos nos artigos 2º, 3º, 4º, 5º, 6º, 7ºe 9º desta Lei Complementar.

VII - o fornecimento de dados financeiros e de pagamentos, relativos a operações de crédito e obrigações de pagamento adimplidas ou em andamento de pessoas naturais ou jurídicas, a gestores de bancos de dados, para formação de histórico de crédito, nos termos de lei específica."

41.
BRASIL, Lei Complementar nº 105, de 10 de Janeiro de 2001. Lei do Sigilo Bancário. 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.html

42.
BRASIL, Banco Central do Brasil, Resolução nº 4.658 de 26 de Abril de 2018. Disponível em: https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50581/Res_4658_v1_O.pdf

43.
BRASIL, Banco Central do Brasil. Resolução Conjunta nº 1 de 4 de maio de 2020. Disponível em: https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/51028/Res_Conj_0001_v1_O.pdf

44.
§ 4º do artigo 5 da Resolução Conjunta nº 1 de 4 de maio de 2020.

45.
EUROPA. EDPS. Guidelines on data protection in EU financial services regulation. p. 5. Disponível em: https://edps.europa.eu/sites/edp/files/publication/14-11-25_financial_guidelines_en.pdf. Acesso em:7 de junho de 2020.

46.
Inciso II do artigo 2, da Resolução Conjunta nº 1 de 4 de maio de 2020.

47.
REYNOLDS, Faith. Open Banking: a consumer perspective. UK Open Banking, p. 18-19, 2017. Disponível em: <https://www.openbanking.org.uk/wp-content/uploads/Open-Banking-A-Consumer-Perspective.pdf>. Acesso em: 16 de maio de 2020.

48.
CUEVA, Ricardo Vilas Boas. A insuficiente proteção de dados pessoais no Brasil. Revista de Direito Civil Contemporâneo-RDCC: Journal of Contemporary Private Law, n. 13, p. 61, 2017.

49.
MARTINS, Leonardo (Org.). Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão. Montevidéu: Fundação Kontad Adenauer, 2005, pp. 233-235

50.
BRASIL, Banco Central do Brasil, Resolução nº 4.658 de 26 de Abril de 2018. Dispõe sobre a implementação do Sistema Financeiro Aberto (Open Banking). Disponível em: https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50581/Res_4658_v1_O.pdf

51.
BRASIL. Escola Nacional de Defesa do Consumidor A proteção de dados pessoais nas relações de

consumo: para além da informação creditícia / Escola Nacional de Defesa do Consumidor; elaboração Danilo Doneda. – Brasília: SDE/DPDC, p. 43, 2010. Disponível em: https: //www. justica.gov.br/seus-direitos/consumidor/Anexos /manual-de-protecao-de-dados-pessoais.pdf. Acesso em: 17 de maio de 2020.

52.
BRASIL. Governo Federal. Guia de Boas Práticas para Implementação na Administração Pública Federal. 1 v. 21, 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf. Acesso em: 16 de maio de 2020.

53.
Idem. p. 26.

54.
FRANCE. European Union Agency for Fundamental Rights. Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights. p. 8, 2019. Disponível em: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf. Acesso em: 17 de maio de 2020.

55.
O GLOBO. Algoritmos reproduzem machismo e racismo por se basearem em práticas discriminatórias dos humanos. Disponível em: https://oglobo.globo.com/economia/algoritmos-reproduzem-machismo-racismo-por-se-basearem-em-praticas-discriminatorias-dos-humanos-24085081. Acesso em: 17 de maio de 2020.

Quais os desafios de implementação do Open Banking frente à LGPD e regulações do BCB?
56.
Resolução Conjunta 1/2020 BCB, Art. 2º, IV - instituição receptora de dados: instituição participante que apresenta solicitação de compartilhamento à instituição transmissora de dados para recepção dos dados do escopo desta Resolução Conjunta.

57.
Resolução Conjunta 1/2020 BCB, Art. 2º, VI - instituição iniciadora de transação de pagamento: instituição participante que presta serviço de iniciação de transação de pagamento sem deter em momento algum os fundos transferidos na prestação do serviço.

58.
Resolução Conjunta 1/2020 BCB, Art. 10º. A instituição receptora de dados ou iniciadora de transação de pagamento, previamente ao compartilhamento de que trata esta Resolução Conjunta, deve identificar o cliente e obter o seu consentimento.

59.
LGPD, Art. 11, O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas.

60.
LGPD, Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular.

61.
Conceito cunhado pela Corte Constitucional Alemã no julgamento da Lei do Censo Alemã de 1983. Nesse sentido, MARTINS, Leonardo. Introdução à jurisprudência do Tribunal Constitucional Federal Alemão. Cinquenta anos de jurisprudência do TCFA. Trad. Beatriz Henning et al. Montevidéu: Fundação Konrad Adenauer, 2005.

62.
BIONI, Bruno Ricardo. Proteção de Dados Pessoais - A Função e os Limites do Consentimento. Forense: Edição do Kindle, p. 113-115, 2019.

63.
Nesse sentido: BIONI, Bruno Ricardo. opt. cit.; SOLOVE, Daniel. Introduction- Privacy self-management and the consent dilemma. Harvard Law Review, 126(7), 1880-1903, 2013; RICHARDS, Neil; HARTZOG, Woodrow. The Pathologies of Digital Consent. 96 Washington University Law Review 1461, 2019; e MONTEZUMA, Luis Alberto; TAUMAN-BASSIRIAM, Tara. How to avoid consent fatigue. IAPP – International Association of Privacy Professionals. 2019. Disponível em <https://iapp.org/news/a/how-to-avoid-consent-fatigue/>. Acesso em: 15 de maio de 2020.

64.
Nesse sentido: BIONI, Bruno Ricardo. opt. cit.

65.
Center For Information Policy Leadership (CIPL). Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Guidelines on Consent". Disponível em: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_wp29_guidelines_on_consent-c.pdf. Acessado em: 11 de maio de 2020.

66.
McDONALD, Aleecia M; CRANOR, Lorrie Faith. The cost of Reading Privacy Policies. A Journal of Law and Policy for the Information Society Volume 4, edição 3, 2009.

67.
SOLOVE. *opt. cit.*

68.
EUROPEAN DATA PROTECTION BOARD. Guidilines on Consent. Adotada em 4 de maio de 2020. Disponível em: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf. Acessado em: 13 de maio de 2020.

69.
Resolução Conjunta 1/2020 BCB, Art. 2º, VIII - consentimento: manifestação livre, informada, prévia e inequívoca de vontade, feita por meio eletrônico, pela qual o cliente concorda com o compartilhamento de dados ou de serviços para finalidades determinadas.

70.
SOLOVE. *opt. cit.*

71.
Resolução Conjunta 1/2020 BCB, Art. 11. Os dados objeto de compartilhamento podem ser apresentados ao cliente de forma agrupada, com base em critérios a serem estabelecidos na convenção de que trata o art. 44. Parágrafo único. Para fins do disposto no caput, o agrupamento de dados deve: I - ser identificado de forma clara, objetiva e adequada; II - possibilitar a discriminação dos dados pelo cliente em nível granular; e III - guardar relação com os dados representados em nível granular.

72.
LGPD, Art. 6º, I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

73.
LGPD, Art. 6º, II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

74.
LGPD, Art. 6º, III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

75.
LGPD, Art. 6º, VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

76.
LGPD, Art. 6º, VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

77.
LGPD, Art. 6º, IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

78.
Resolução Conjunta 1/2020 BCB, Art. 40, Art. 40. As instituições de que trata o art. 1o devem instituir mecanismos de acompanhamento e de controle com vistas a assegurar a confiabilidade, a disponibilidade, a integridade, a segurança e o sigilo de que tratam os arts. 31 e 39, bem como a implementação e a efetividade dos requisitos de que trata esta Resolução Conjunta, incluindo: I - a definição de processos, testes e trilhas de auditoria; II - a definição de métricas e indicadores compatíveis; e III - a identificação e a correção de eventuais deficiências.

79.
NETDILIGENCE. Cyber Claims Study. Report, 2019. Disponível em: https://netdiligence.com/wp-content/uploads/2020/03/2019_NetD_Claims_Study_Report_1.2.pdf. Acessado em: 15 de maio de 2020.

80.
BCB, Resulução Nº 4.658/2018 e Circular Nº 3.909/

2018, Art. 2º, as instituições de pagamento e financeiras devem implementar e manter política de segurança cibernética formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados, § 1o A política mencionada no caput deve ser compatível com: I - o porte, o perfil de risco e o modelo de negócio da instituição.

81.
MCKINSEY & COMPANY. Data sharing and Open Banking. McKinsey on Payments, p. 4, 2017. Disponível em: <https://www.mckinsey.it/sites/default/ les/data- sharing-and-open-banking.pdf>. Acesso em: 13 de maio de 2020.

82.
BCB, Resolução Nº 4.658/2018 e Circular Nº 3.909/2018, Art. 3º. A política de segurança cibernética deve contemplar, no mínimo: II - os procedimentos e os controles adotados para reduzir a vulnerabilidade da instituição de pagamento a incidentes e atender aos demais objetivos de segurança cibernética; § 3o Os procedimentos e os controles citados no inciso II do caput devem ser aplicados, inclusive, no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias empregadas nas atividades da instituição de pagamento.

83.
RUBINSTEIN, Ira; GOOD, Nathan. Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents. Berkeley Technology Law Journal n. 28, 2013.

84.
LGPD, Art. 46, os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. § 2o As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

85.
VRIJE UNIVERSITY OF BRUSSELS. Personal data protection in the financial sector. Data Protection on the Ground: round table report, 2019, p.3. Disponível em: https://smit.vub.ac.be/wp-content/uploads/2020/01/Report-roundtable-data-protection-in-the-financial-sector_def.pdf. Acessado em: 9 de maio de 2020.

86.
Ibidem.

87.
Ibidem.

88.
LGPD, Art. 55-J, Compete à ANPD: XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação.

89.
LGPD, Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.

Quais as eficiências e os entraves econômicos para as empresas que adotarem o Open Banking?
90.
BRODSKY L, OAKES L. Data Sharing and Open Banking. McKinsey on Payments. https://www.mckinsey.it/sites/default/files/data-sharing-and-open-banking.pdf. Published 2017. Accessed April 19, 2020.

91.
IMF. Financial Access Survey. https://data.imf.org/?sk=E5DCAB7E-A5CA-4892-A6EA--598B5463A34C&sId=1390030341854. Published 2020. Accessed May 14, 2020.

92.
IMF. Financial Development Survey. https://data.imf.org/?sk=F8032E80-B36C-43B1-AC26-493C5B-1CD33B&sId=1481126573525. Published 2020. Accessed May 14,2020.

93.
As imagens foram geradas pelos autores, a partir dos dados obtidos pelos relatórios do FMI.

94.
BROWN-HRUSKA, Sharon; ELLIG, Jerry. Financial Markets as Information Monopolies?. CATHO Institute, vol. 3, 2000. Disponível em: <https://www.cato.org/sites/cato.org/files/serials/files/regulation/2000/10/ellig.pdf>. Acesso em: 12 set. 2020.

95.
HALLSWORTH J, RUARK R, POLLARI I. Open Banking Opens Opportunities for Greater Customer Value: Reshaping the Banking Experience; KPMG, 2019.

96.
BRODSKY L, OAKES L, op. cit., p. 8.

97.
HALLSWORTH J, RUARK R, POLLARI I, op. cit., p. 3-4.

98.
REYNOLDS, Faith. Open Banking: a consumer perspective (Issue January). Barclay, 2017, p. 12. Disponível em: <https://home.barclays/content/dam/home-barclays/documents/citizenship/access-to-financial-and-digital-empowerment/Open-Banking-A-Consumer-Perspective-Faith-Reynolds.pdf>. Acesso em: 12 set. 2020.

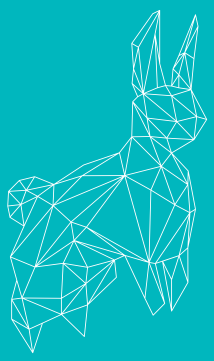
99.
Ibid, p. 13.

100.
Ibid, p. 14.

101.
Ibid, p. 18.

102.
IMF. Financial Development Survey. https://data.imf.org/?sk=F8032E80-B36C-43B1-AC26-493C5B-1CD33B&sId=1481126573525. Published 2020. Accessed May 14,2020.

Conclusão
103.
Ibid.



LAPIN