NOVEMBRO, 2020

Open Banking e Proteção de Dados

AUTORES

Mario Viola

Leonardo Heringer

Janaina Costa

EDITORAÇÃO E REVISÃO

Celina Bottino

Christian Perrone

GREAT for PARTNERSHIP

BRITAIN & NORTHERN IRELAND

ITS

Instituto de Tecnologia & Sociedade do Rio

SUMÁRIO

1. INTRODUÇÃO

Quando se imaginava o futuro nos fins do século passado, a ideia de que pessoas pagariam contas, cuidariam de suas finanças e fariam transações bancárias online, parecia objeto de ficção científica. No entanto, a velocidade com que houve uma transformação de um passado não muito distante em que dados eram analógicos - em que coletar ou compartilhar informações significava lidar com documentos físicos - para o mundo digital é impressionante. Nesse contexto, o fenômeno da hiperconectividade[1] está mudando a maneira como os negócios são feitos e incentivam as empresas a repensar tudo, incluindo como operam e entregam valor aos seus clientes. As projeções para o impacto na economia deste cenário de hiperconexão são impressionantes - estima-se um acréscimo na economia global de mais de US$ 11 trilhões em 2025[2].

O sistema financeiro é um desses setores em franca mutação e com mercado em expansão. O Banco Mundial estima que existem cerca de 1,7 bilhão de adultos no mundo sem acesso a serviços financeiros e ao crédito[3]. No Brasil esse número corresponde a 45 milhões de pessoas, um terço da população de brasileiros adultos que ainda ainda que não bancarizados movimentam mais de R$ 800 bilhões por ano.[4] Por outro lado, na experiência digital, os consumidores têm baixa tolerância a inconveniências e esperam serviços altamente intuitivos e eficientes.[5]

Esses fatores impelem a uma revolução na maneira como as empresas de serviços financeiros desenvolvem e distribuem seus produtos. É preciso encontrar meios para suprir a demanda dos desbancarizados e também inovar para solucionar os gargalos encontrados pelo sistema bancário tradicional, como a aprovação de crédito mais rápida e menos burocrática e o uso da tecnologia para melhorar a experiência do cliente.

Nessa conjuntura, nos deparamos com um paradoxo no país. O Brasil possui um efervescente ecossistema de inovação financeira - o maior ecossistema Fintech da América Latina em 2018.[6] Todavia, o Relatório de Economia Bancária do Banco Central informa que apenas 5 bancos concentram mais de 80 % do mercado de crédito e depósitos totais nacionais.[7]

É nesse cenário que o setor financeiro alcança o próximo nível de evolução: a era do *open banking*. Essa é a denominação internacional para a versão aberta do sistema financeiro, que se beneficia do processo de digitalização. Tudo isso graças às oportunidades que surgem no campo de dados - muitos desses pessoais.

No caso do Brasil, após um período de discussões em que partes da sociedade puderam se manifestar, o *open banking* foi regulamentado pelo Conselho Monetário Nacional e pelo Banco Central do Brasil, através da Resolução Conjunta nº 01/2020, e deverá estar totalmente implementado até o final de 2021.

Enquanto a participação das instituições financeiras, o sistema é pensado para ser aberto inclusive nesse sentido. As instituições maiores, enquadradas nos Segmentos 1 (S1) e 2 (S2)[8] serão obrigadas a participar.[9] Outras instituições *poderão* se juntar ao sistema e espera-se que em grande medida o façam para tornar o sistema mais robusto e abrangente.

De acordo com a regulamentação nacional, o *open banking* caracteriza-se pelo *"compartilhamento padronizado de dados e serviços por meio de abertura e integração de sistemas"*,[10] com o objetivo de ***(i)*** incentivar a inovação; ***(ii)*** promover a concorrência; ***(iii)*** aumentar a eficiência do Sistema Financeiro Nacional e do Sistema de Pagamentos Brasileiros e; ***(iv)*** promover a cidadania financeira.[11]

Quanto à sua origem, de acordo com o Banco Central do Brasil, o *open banking* se ampara na convicção *"de que os dados bancários pertencem aos clientes e não às instituições financeiras".*[12] O impacto dessa assertiva é enorme, pois permite que uma miríade de informações financeiras fiquem disponíveis à conveniência dos clientes. Isso significa, como se tratará na seção seguinte, a quebra de uma importante barreira de entrada no mercado.

No centro dessa transformação resta a proteção dos dados pessoais. A regulação da proteção de dados, mais do que uma norma garantidora de direitos, torna-se pedra de toque para que consumidores confiem no comércio eletrônico e nos diferentes serviços digitais que daí surgem. Além disso, essa normativa também tem o efeito de fomentar novos negócios,[13] novos modelos, e estimular a inovação. A LGPD (Lei geral de proteção de Dados - Lei 13.709 de 2018) serve, pois, como um instrumento de segurança jurídica, informando, a quem busca utilizar dados pessoais, como esses podem ser utilizados e sob quais fundamentos.

Por outro lado, instituir normas de privacidade e proteção de dados que busquem paridade com sistemas internacionais como o GDPR (Regulamento Geral sobre a Proteção de Dados da União Europeia), tal como a nossa LGPD , inclui o país nos mercados que fazem uso de dados pessoais e exigem um nível de adequação semelhante. Igualmente, a sanção da legislação protetiva dos dados pessoais também é etapa importante para a participação na OCDE (Organização para Cooperação e Desenvolvimento Econômico), que permite acesso a mercados e facilita negócios. Não por acaso, 66% dos países do globo já regulamentaram proteção de dados pessoais e privacidade[14].

O presente relatório pretende chamar a atenção a importância central da proteção de dados para uma série de oportunidades para o Brasil e para a região. A recente entrada em vigor da Lei Geral de Proteção de Dados Pessoais representa sim mais do que a concretização de direitos para cidadãos e consumidores; um verdadeiro momento chave para expandir um setor que já está em desenvolvimento que é o de Fintechs - tecnologia

aplicada ao setor de finanças – o qual, cresceu 66% (sessenta e seis por cento) na América Latina e no Caribe em um ano,segundo os dados do "Relatório Fintech América Latina 2018: Crescimento e Consolidação"[15], produzido pelo Banco Interamericano de Desenvolvimento. A proteção de dados, então, torna-se um mecanismo que facilita e permite que todo um setor da economia brasileira ganhe novos contornos e seja energizado. É dentro desse contexto que se analisará como a proteção de dados e o *open banking* podem revolucionar o ecossistema de inovação financeira no Brasil. Utilizar-se-á duas perspectivas distintas, a da proteção de dados e a da concorrência.

A estrutura proposta é, em um primeiro momento, demonstrar como a proteção de dados e o *open banking* são complementares e têm o condão de alavancar o ecossistema de inovação financeira no Brasil. Para tanto, a experiência europeia e, particularmente, do Reino Unido, servem de referências.

Adicionalmente, analisar-se-á os desafios práticos e regulatórios que o sistema instituído no Brasil trás. Finalmente, mirando ao futuro, expor-se-á a complexidade regulatória trazida pelo sistema pensado do ponto de vista do setor econômico, mas cuja centralidade nos dados torna necessária a harmonização das competências dos órgãos do setor econômico com as funções da Autoridade Nacional de Proteção de Dados (ANPD) estabelecida na LGPD.

Esse é o primeiro de uma série de dois relatório sobre *open banking*. Neste analisaremos a oportunidade trazida por um sistema saudável de proteção de dados para a instituição do *open banking*. Em um segundo relatório analisar-se-á de maneira mais aprofundada a questão da portabilidade dados e a interoperabilidade de sistemas como pontos cardeais do sistema financeiro aberto.

2. *OPEN BANKING*: CONCORRÊNCIA, PROTEÇÃO DE DADOS E O ECOSSISTEMA DE INOVAÇÃO

Do ponto de vista brasileiro, o mercado financeiro sempre foi muito tecnológico, mas tendendo a ser bastante concentrado.[16] Dois elementos parecem favorecer essa visão. Primeiro, a atividade do setor de finanças tende a convergir na atuação de bancos, o que leva a uma restrição da mesma em grandes instituições com licença para operar.[17] Além do mais, historicamente, bancos estiveram na vanguarda no uso de tecnologia tendo sido os primeiros a se utilizar em larga escala de tecnologias de comunicação - implementaram o telégrafo, o telefone, computadores (e caixas automáticos) e mais recentemente tecnologias da informação como um todo.[18]

Um segundo elemento se relaciona ao fato do setor de finanças estar baseado na guarda, transmissão e trato de informação. Em sua incepção, a

lógica do sistema financeiro se dá na capacidade de intermediar relações econômicas entre as pessoas (e empresas), o que tem como base o processamento de transações e a guarda meticulosa de anotações sobre elas. Desse modo, instituições financeiras tendem a construir vastos bancos de dados consolidando muita da atividade econômica de seus clientes. Isso permite que tenham importantes *insights* sobre os hábitos de seus clientes além de sua saúde financeira, permitindo que lhes ofereçam serviços específicos para as suas necessidades.

A crise do setor em 2008 – que se inicia com a falência do Banco Lehmann Brothers – estimula uma mudança no paradigma de centralização tecnológica e de informações (dados pessoais).[19] Um alinhamento de fatores econômicos e tecnológicos que permite que novos atores adentrem ao mercado (startups de finanças - fintechs majoritariamente) e busquem novos modelos de negócio e novas oportunidades de prestar serviços financeiros.[20] Esses têm como ponto inicial uma mudança significativa nos meios de pagamento, mas de maneira nenhuma ficam restritos a esses.[21] Essas novas empresas, muitas originalmente de menor porte, passam a atuar no mercado financeiro, concorrendo com grandes atores já estabelecidos e concentradores de dados de seus consumidores.

Nesse sentido, o elemento de acesso à tecnologia diminui de relevância como uma vantagem competitiva. Os novos atores, por não dependerem de um legado de infraestrutura, podem inclusive ser mais rápidos na adaptação de seus sistemas e na incorporação de novas tecnologias. No entanto, por serem atores mais novos, menores e menos consolidados não possuem o mesmo acesso à vasta quantidade de informações disponível. Os dados coletados e armazenados pelas empresas com presença já mais efetiva no mercado passam, então, a ser hoje uma das maiores barreiras de entrada[22] de novos competidores.

O *open banking* e a liberdade que será conferida ao consumidor no uso dos seus dados pessoais têm a possibilidade de servir como meio de mitigação desse obstáculo. A proteção de dados traz além de uma maior segurança jurídica sobre o uso de dados pessoais, também potenciais ganhos concorrenciais que permitirão não só o ingresso de novos atores, mas a transformação do ecossistema dando maior acessibilidade aos usuários e promovendo uma mudança no comportamento dos atores já existentes.[23]

Em suma, em uma economia digital, poder passar de um serviço para outro se torna um fator-chave para a concorrência de mercado e garantir a escolha e a proteção do consumidor. O direito à portabilidade, previsto na LGPD, na GDPR e em outras normativas, facilita aos usuários não ficarem adstritos ao seu serviço tradicional, podendo escolherem os serviços que melhor se adaptam às suas necessidades.

O sistema financeiro aberto, está nessa mesma linha. Tem como alicerce a escolha do consumidor, em consonância com uma autodeterminação informativa com relação a seus dados. O sistema está, então, ligado ao direito à portabilidade de dados pessoais, partindo de uma mesma compreensão de que os dados bancários são de seus titulares e as instituições financeiras somente os podem utilizar de acordo com a normativa de proteção de dados pessoais.

Nesse sentido, Rafael Zanatta e Ricardo Abramovay, ao analisarem os problemas emergentes relacionados aos poderes das grandes empresas de tecnologia que atuam na camada de aplicações de internet e que se dedicam, direta ou indiretamente, à exploração de dados pessoais, chegam a uma previsão otimista. Destacam que o direito a proteção de dados tem esse condão de revolucionar o direito concorrencial. Isto porque a seu ver, no contexto do *open banking* estruturado pelo Banco Central do Brasil, o direito à portabilidade de dados pode

> *fomentar a circulação de dados pessoais desde que exista o consentimento e o pedido por parte do titular dos dados, fazendo que grandes instituições financeiras sejam obrigadas a garantir acesso a competidores (FinTechs), estimulando uma espécie de desagregação (unbundling) dos serviços financeiros hoje unificados.*[24]

O presidente da Associação Brasileira de Fintechs (ABFintechs), Diego Perez, compartilha desse otimismo e declarou acreditar que com a regulamentação do *open banking* o número de Fintechs irá dobrar no país, passando das 720 existentes para mais de 1400.[25]

Ainda a respeito dos possíveis proveitos concorrenciais que poderão advir da adoção desse sistema aberto de compartilhamento de dados, interessante observar as colocações de Paula de Andrade Baqueiro e Paula Farani de Azevedo Silveira:

> *De fato, do ponto de vista concorrencial, a proposta poderá gerar impactos bastante relevantes para ampliar e acirrar a competição no setor financeiro, na medida em que o open banking facilitará o acesso e fluxo de dados, hoje tidos como elementos centrais para movimentar a entrada e as inovações no setor.*
>
> *Atualmente, em nível global, o sistema financeiro é reconhecido como um setor marcado por altas barreiras à entrada, baixa elasticidade da demanda, efeitos de rede e de trancamento (lock-in), e práticas de abuso de posição dominante pelos incumbentes. Associado a essas carac-*

> *terísticas, verifica-se ainda um fenômeno generalizado de verticalização, que acaba por fomentar um cenário propício à realização de práticas de venda casada (tying), uma vez que os agentes passam a atuar em vários elos da mesma cadeia produtiva ou em mercado correlatos, promovendo um ambiente de poder conglomerado pelos incumbentes.*[26]

Como destacam as autoras acima citadas, de fato:

> *Esses fatores, aliados ao próprio dinamismo e caráter disruptivo do setor, findam por tornar o sistema financeiro, em sentido amplo, um alvo constante de investigações por condutas anticompetitivas no Conselho Administrativo de Defesa Econômica (CADE).*
>
> *A implementação do Sistema Financeiro Aberto tem o potencial de alterar a dinâmica competitiva do setor, uma vez que é capaz de atenuar o chamado "problema do gargalo de dados" (data bottleneck problem), que dificulta e atrasa a entrada efetiva de novos agentes em mercados movidos a dados, tal como o financeiro.*[27]

Somado a isso, é importante ressaltar que a regulamentação da proteção de dados tem ainda o potencial de fomentar o ecossistema de inovação financeira, expandir e criar novos modelos de negócio. As empresas, setor financeiro incluso, deverão garantir que os dados pessoais sejam processados de forma adequada e incorporar o quanto antes as novas necessidades desse novo cenário de privacidade e proteção de dados na estratégia de seus negócios. Para tanto, avanços tecnológicos e revisão de processos serão fundamentais para reduzir os encargos administrativos e as cargas de trabalho manuais.

Analistas financeiros, como da Gartner, preveem que os gastos no mundo voltados à privacidade e proteção de dados em ferramentas de conformidade alcançarão 8 bilhões de dólares até 2022.[28] Isso significa a emergência de um novo modelo de negócio – *privacy as a business model* – e o surgimento de uma miríade de novos serviços e tecnologias. Nesse sentido, já desponta, por exemplo, a tendência de uso de Inteligência Artificial (IA) no setor.[29]

O *open banking* é, todavia, mais do que um mero instrumento de correção de vicissitudes concorrenciais e oportunidade de inovação. O seu propósito é maior. É necessário enxergar o consumidor, titular dos dados e destinatário dos serviços que serão compartilhados, como o elemento central desse sistema, pois é para ele, afinal, que deve servir o funcionamento eficiente do mercado.

Essa menção ao compartilhamento, aliás, é para guardar coerência com a proclamada visão do Banco Central do Brasil[30] sobre o *open banking*, uma vez que sendo a autodeterminação informativa do consumidor a base de criação do sistema financeiro aberto, é certo que além do compartilhamento de dados, produtos e serviços, também será possível utilizar a interoperabilidade dos sistemas para fins de portabilidade, apesar de a primeira não necessariamente dar ensejo à segunda. O que o *open banking* enseja é o compartilhamento de dados pelos diversos agentes envolvidos,[31] que ocorrerá a cada nova transação enquanto viger a autorização dada pelo consumidor, enquanto a portabilidade dos dados é direito do titular do dado criado pela LGPD e que importa na transferência dos seus dados pessoais para outro fornecedor.

Sob essa ótica, impõe-se a adoção de medidas efetivas de proteção dos dados pessoais do consumidor, posto que a interoperabilidade dos sistemas apregoada pelo *open banking*, a ser adotada a partir do emprego de APIs *(application programming interfaces)*[32] abertas[33] ocasionará um expressivo aumento no volume de informações que serão compartilhadas eletronicamente, o que demandará mecanismos eficazes de segurança.

A segurança dos dados tem sido uma preocupação na implementação do *open banking* em outras partes do mundo[34] e se torna especialmente necessária no modelo brasileiro, dado o crescente índice de criminalidade cibernética[35] que tem se observado no país.

Precisamente em razão desses potenciais riscos é que a regulamentação do *open banking* alçou a *"segurança e privacidade de dados e de informações sobre serviços compartilhados"* dentre os seus princípios norteadores[36] e estabeleceu diversas regras concernentes à segurança (art. 8º, parágrafo único, inciso I[37]; art. 18[38]; art. 31[39]; art. 33, §1º, inciso III[40]; art. 38, inciso IV e §3º[41]; art. 39[42]; art. 40 ***caput*** e §2º, inciso II[43]; art. 44, inciso I, "a", item 4, "b"[44]; art. 48, inciso III[45]).

Portanto, além de um importante instrumento de aperfeiçoamento de mercado, o *open banking* deve ser entendido como a expressão da autodeterminação informativa do consumidor, que deverá ter a certeza de que seus dados pessoais estarão protegidos.

3. A EXPERIÊNCIA EUROPEIA E DO REINO UNIDO

No âmbito da União Europeia, os sistemas de pagamentos interoperáveis[46] foram regulamentados no ano de 2012, através do Regulamento (UE) nº 260/2012, com a finalidade de estimular a concorrência e racionalizar o funcionamento do mercado interno do Bloco.[47]

Persistindo nessa ideia - de integração dos meios de pagamentos dentro do Bloco, poucos anos após, foi aprovada a Diretiva (UE) nº 2015/2366, também conhecida como PSD2 (*Second Payments Services Directive).*

Esta estabeleceu orientações mais ambiciosas no sentido de tornar interoperáveis os sistemas de dados e estimular novos participantes nesse mercado, inclusive os chamados *third party payment providers*[48]. Nesse contexto, o objetivo era proporcionar uma estrutura simples em que diferentes participantes poderiam operar e que o mercado como um todo prosperasse, melhorando a situação do consumidor e estimulando a inovação e a criatividade.

Aprofundando ainda mais essa intenção integrativa, no Reino Unido[49] o CMA *(Competition and Markets Authority)* publicou no ano de 2016 um documento intitulado *"making banks work harder for customers".*[50] Neste propõe-se a base do que hoje é o OBIE *(Open Banking Implementation Entity),* empresa criada pelos nove maiores bancos britânicos com a atribuição de coordenar as medidas para a implementação do *open banking*.[51]

A sistemática criada no Reino Unido leva a um aporte maior da participação dos próprios entes privados que devem facilitar ou promover um ecossistema de maior competição para si mesmos. Não é então dependente de um órgão público, ainda que estes - como a CMA - supervisionem o seu funcionamento.

A lógica do sistema é desde a origem permitir um maior fluxo de informações a serem compartilhadas em decorrência da adoção de sistemas abertos e interoperáveis. Estimular a concorrência, mas também permitir mais diversidade e potencialmente melhores escolhas para os consumidores, além do exercícios de seus direitos. A proteção de dados pessoais passa a ter um papel crucial nesta faculdade de favorecer a interoperabilidade.

O modo como esse sistema financeiro foi estruturado no Reino Unido foi para criar interfaces nas quais diferentes instituições poderiam desenvolver novos produtos e serviços para os usuários de serviços financeiros.[52] Nesse sentido, existe um necessário acesso a dados importantes dos participantes.

Esta centralidade do acesso e proteção a dados pessoais já estava presente no PSD2, que explicita em diversas passagens a necessidade de respeitar as regras de proteção de dados pessoais, como se observa, por exemplo, do teor do seu considerando nº 89, *verbis:*

> *A prestação de serviços de pagamento pelos prestadores de serviços de pagamento pode implicar o tratamento de dados pessoais. A Diretiva 95/46/CE do Parlamento Europeu e do Conselho, as regras nacionais que transpõem a Diretiva 95/46/CE e o Regulamento (CE) nº 45/2001 do Parlamento Europeu e do Conselho são aplicáveis ao tratamento de dados pessoais para efeitos da presente diretiva. Em especial,* caso os dados pessoais sejam tratados para efeitos da presente diretiva, deverá ser especificado o objetivo exato, deverá ser referida a base

> jurídica aplicável, deverão ser cumpridos os requisitos de segurança aplicáveis estabelecidos na Diretiva 95/46/CE e deverão ser respeitados os princípios da necessidade, da proporcionalidade, da limitação da finalidade e do período proporcionado de conservação de dados. De igual modo, a proteção de dados desde a concepção e a proteção de dados por defeito deverão estar incorporadas em todos os sistemas de tratamento de dados desenvolvidos e utilizados no quadro da presente diretiva. *(sem grifos no original)*

Aliás, importante notar que essa preocupação com a proteção de dados pessoais vem aumentando, levando o Comitê Europeu para Proteção de Dados (EDPB – *European Data Protection Board)* a colocar recentemente em consulta pública (julho de 2020) o texto das *"Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR"*[53], esclarecendo o seguinte:

> *The second Payment Services Directive (hereinafter "PSD2") has introduced a number of novelties in the payment services field. While it creates new opportunities for consumers and enhances transparency in such field, the application of the PSD2 raises certain questions and concerns in respect of the need that the data subjects remain in full control of their personal data. The General Data Protection Regulation (hereinafter "GDPR") applies to the processing of personal data including processing activities carried out in the context of payment services as defined by the PSD2. Thus, controllers acting in the field covered by the PSD2 must always ensure compliance with the requirements of the GDPR, including the principles of data protection set out in Article 5 of the GDPR, as well as the relevant provisions of the ePrivacy Directive. While the PSD2 and the Regulatory Technical Standards for strong customer authentication and common and secure open standards of communication (hereinafter "RTS") contain certain provisions relating to data protection and security, uncertainty has arisen about the interpretation of these provisions as well as the interplay between the general data protection framework and the PSD2.*

Dessa forma, como se observa, o *open banking* tem sua origem na expansão da sistemática de serviços de pagamentos com maior interopera-

bilidade de sistemas e com uma pedra de toque no acesso a dados. Ganha contornos mais amplos com a estruturação do sistema pela visão trazida pelo Reino Unido. Dessa forma, ampliando a interoperabilidade de serviços, para um sistema aberto em que se pode inovar na prestação de serviços financeiros. Permite também ganhos do ponto de vista de concorrência por diminuir as barreiras de entrada e permitir novos atores ter acesso a consumidores e aos elementos relevantes (informações) para a prestação destes serviços.

Conforme vem demonstrando a experiência europeia, os ganhos potenciais são amplos, mas não podem ser desprezados os riscos que a adoção desse sistema traz para a proteção dos dados pessoais, os quais serão tratados logo abaixo.

4. CENTRALIDADE DA PROTEÇÃO DE DADOS

O sistema financeiro aberto está alicerçado na proteção de dados e na autodeterminação informativa. Corrobora essa constatação o teor do voto proferido[54] pelo Diretor de Regulação do Banco Central do Brasil, que ao propor a aprovação da regulamentação do *open banking* consignou o seguinte:

> *Em comum, tais ações [open banking em outros lugares do mundo] geralmente têm por objetivo aumentar a competitividade nos mercados financeiros, incentivar a inovação financeira, racionalizar os processos de instituições reguladas, possibilitar parcerias comerciais entre instituições financeiras e instituições não financeiras, e, também, em diversos casos,* empoderar o consumidor financeiro*. Importante ressaltar que* o consumidor é reconhecido como o titular dos seus dados pessoais*; no caso do Brasil a Lei Geral de Proteção de Dados Pessoais (LGPD), a Lei nº 13.709, de 14 de agosto de 2018, reforçará e sistematizará, a partir de sua entrada em vigor, a tutela desses dados.* Com o *Open Banking*, o consumidor financeiro pode consentir com o compartilhamento padronizado de dados e serviços por meio de abertura e integração de sistemas de instituições financeiras e de pagamento, caso vislumbre algum benefício com esse compartilhamento, a exemplo do acesso a serviços financeiros adequados ao seu perfil*. (sem grifos no original)*

Logo, se o que o *open banking* declaradamente busca é o empoderamento do consumidor, deve, por coerência, tê-lo como o seu elemento mais importante. Não faz sentido utilizar a autodeterminação informativa do consumidor como argumento de criação do sistema, mas concebê-lo

sob um viés exclusivamente de mercado, sem se preocupar com a proteção dos seus dados.

E foi exatamente por isso que, conforme mencionado anteriormente, o regulamento do *open banking* brasileiro se preocupou em estabelecer inúmeras regras de segurança e proteção dos dados que serão compartilhados, como se extrai da Resolução Conjunta nº 01/2020 do Banco Central do Brasil e do Conselho Monetário Nacional, da qual trataremos no próximo tópico. Parece que a (correta) ideia que se buscou transmitir é a de que a proteção dos dados pessoais tem um papel central no *open banking*.

Não se minimiza, absolutamente, a importância dos ganhos econômicos / concorrenciais que decorrerão da implementação do sistema financeiro aberto, mas é necessário enxergar o *open banking* e interpretar as regras de sua regulamentação não como a de um simples instrumento de aperfeiçoamento do ambiente concorrencial. É essencial que o sistema, destinado ao empoderamento do consumidor, ofereça segurança e funcione em conformidade com as regras sobre proteção de dados pessoais, em especial a Lei Geral de Proteção de Dados Pessoais (LGPD).

4.1. O consentimento e as demais bases legais para o tratamento dos dados pessoais:

O tratamento de dados pessoais pressupõe a existência de uma base legal que o autorize. Levando em consideração que central à estrutura do de *open banking* está a transferência de dados pessoais, resta claro que deve existir uma base legal que justifique e legitime essa transferência.

Ainda que a discussão sobre *open banking* tenha se iniciado no Brasil antes da vigência da Lei Geral de Proteção de Dados Pessoais (LGPD), o sistema foi pensado em um contexto em de crescente preocupação com a matéria. Sendo assim , a normativa estabelece o consentimento do consumidor (titular de dados) como a base autorizativa por excelência que possibilita a transmissão de dados que caracteriza o sistema. Define inclusive esse consentimento como sendo a *"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".*[55] Essa, em verdade, está em harmonia e resta como um detalhamento da definição trazida pelo inciso XII do art. 5º da LGPD. A resolução tem a peculiaridade de especificar que o meio pelo qual deve ocorrer a expressão do consentimento no caso do *open banking* é o o eletrônico.

Na lógica, trata-se de um sistema que possui pelo menos três atores: o consumidor (titular de dados), uma instituição financeira receptora (que requer os dados), e uma instituição fornecedora (que detém os dados e que os pode prestar). Nessa lógica de três pontas, de acordo com as regras estabelecidas na resolução, *"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".[56]

Nesse sentido, o compartilhamento de dados em caso de *open banking*, conforme previsto no §1º do art. 10 da Resolução Conjunta nº 01/2020 do Banco Central do Brasil e do Conselho Monetário Nacional, dependerá sempre de prévio consentimento, que deverá ***(i)*** utilizar linguagem clara, objetiva e adequada; ***(ii)*** ter finalidades determinadas; ***(iii)*** ter prazo de validade compatível com as finalidades, limitado a doze meses; ***(iv)*** discriminar a instituição transmissora de dados ou detentora da conta; ***(v)*** discriminar os dados ou serviços que serão compartilhados; ***(vi)*** identificar o titular dos dados; ***(vii)*** ser posterior à data de vigência do regulamento.

Isso não significa, porém, que todos os tratamentos de dados que se sucederão ao compartilhamento se justificarão com base nesse consentimento.

Basta pensar, a título de exemplo, a hipótese de a instituição receptora precisar, para fins de cumprimento de uma obrigação legal, manter armazenado algum dado pessoal do cliente. Nessa situação, é razoável supor que esse tratamento seguinte (armazenamento do dado) não dependerá do consentimento do titular e estará respaldado em outra base legal prevista na LGPD.

Outro ponto a ser considerado é que o consentimento é a única base a autorizar o compartilhamento de dados bancários dentro do *open banking*, o que não quer dizer que não poderá ocorrer compartilhamento desses mesmos dados em outro ambiente e para outras finalidades, amparadas por outras bases legais, inclusive que dispensam o consentimento do titular, como, por exemplo, a prevenção a fraude, ou mesmo ao crime de lavagem de dinheiro, o que decorre de uma obrigação legal (Lei nº 9.613/98).

Portanto, o consentimento será a única base a legitimar o compartilhamento de dados para fins de utilização do *open banking* do ponto de vista da requisição de dados pessoais. É possível também que sejam realizados tratamentos de dados subsequentes pelas instituições receptoras, desde que relacionados às finalidades informadas ao consumidor e que respeitem as regras da LGPD.

Do ponto de vista da instituição que está fornecendo os dados, aqui trata-se de uma situação um tanto quanto peculiar. A instituição controla os dados do titular, mas deve arcar com a transferência (realizar tratamento) sempre e quando a instituição receptora solicitar – com base no consentimento do titular. Nesse sentido, a receptora tem como base legal o consentimento, mas a fornecedora tem a obrigação legal de realizar a transferência. Ela mesma não precisa obter o consentimento. E frise-se que a despeito de suas obrigações legais advindas de ser controladora os dados pessoais, não deve questionar a entrega dos dados quando requeridos dentro do sistema de *open banking*.

5. DIREITOS DOS TITULARES

Quanto aos direitos assegurados aos titulares dos dados compartilhados no *open banking*, destacam-se aqueles previstos na regulamentação, dos quais é importante notar o de conhecer detalhes dos compartilhamentos realizados (art. 14) e a possibilidade de revogar o consentimento a qualquer tempo (art. 15). Esses direitos decorrem, respectivamente, do princípio da transparência e da autodeterminação informativa. Há um paralelismo importante entre os direitos presentes na LGPD e o que é garantido na regulamentação de *open banking*.

Relativamente aos dados pessoais envolvidos na sistemática de transferências de dados para o *open banking*, aplicam-se, ainda, todos os demais direitos previstos na LGPD, tais como: ***(i)*** o de obter a confirmação da existência de tratamento; ***(ii)*** o de ter acesso aos dados; ***(iii)*** o de corrigir os dados incompletos, inexatos ou desatualizados; ***(iv)*** o de solicitar a anonimização, o bloqueio ou a eliminação de dados desnecessários, excessivos ou tratados em desconformidade com as regras legais; ***(v)*** o da portabilidade; ***(vi)*** o de eliminar em algumas situações os dados tratados em razão do consentimento; ***(vii)*** o de obter informações sobre os compartilhamentos realizados; ***(viii)*** o de obter informações sobre a possibilidade de não conceder o consentimento e as consequências da negativa; ***(ix)*** a revogação do consentimento.[57]

Como se verifica, há um robusto rol de direitos que viabiliza a efetiva proteção dos dados pessoais que serão compartilhados no *open banking*. Caberá ao consumidor ter consciência para poder exercê-los, mas também à futura Autoridade Nacional de Proteção de Dados e ao Banco Central do Brasil fiscalizar a correta aplicação das normas tanto previstas na LGPD quanto específicas do *open banking* pelos atores deste mercado.

Um elemento de suma importância será a implementação técnica desses direitos. No processo de implantação que ainda ocorrer - lembrando que o sistema foi estruturado em 4 fases que devem se finalizar em finais de 2021, os participantes em conjunto com as autoridades devem acordar em como esses direitos devem ser disponibilizados aos titulares. Há uma clara facilitação para requerer a portabilidade. Há um interesse comum das instituições participantes no sistema na portabilidade. Já os incentivos são menores para o exercício de outros direitos como o da revogação do consentimento ou mesmo de corrigir os dados.

Nesse contexto, em sua função de supervisão, os órgãos e autoridades envolvidas devem se atentar que na parte técnica estrutural (nas sugestões dos elementos de estruturação da arquitetura)[58] apareça uma recomendação de que a mesma facilidade para se permitir o consentimento também exista para retirá-lo.[59] Não é uma obrigação expressa pela LGPD, mas é uma decorrência lógica de que a possibilidade de exercício dos direitos seja

acessível e fácil para os titulares de dados. Além disso, a LGPD estabelece a necessidade de ser disponibilizado um canal de comunicação fácil para o titular entrar em contato como encarregado de proteção de dados (art. 41 e ss, LGPD).

5.1. Portabilidade, direitos de terceiros e *open banking*

Dentre os direitos assegurados aos titulares dos dados pessoais, o da portabilidade talvez seja o que suscite maior controvérsia, principalmente no que concerne à delimitação dos dados portáveis e a preservação de direitos de terceiros.

O direito à portabilidade, de acordo com o que dispõe a LGPD[60], pode ser exercido pelo titular dos dados, observados, porém, os segredos comercial e industrial. Ainda que não definido pelo sistema, entende-se que provavelmente não deverão estar no escopo da portabilidade, como também não integram os compartilhamentos que serão realizados pelo *open banking* (art. 5º, §4º, I, "b"), os dados considerados inferidos e derivados[61] – que são aqueles gerados ou complementados a partir de tratamentos realizados pela instituição controladora e constituem o seu *know-how* (inteligência artificial, algoritmos etc).

Essa distinção entre dado pessoal, dado inferido e dado derivado é importante para evitar que ocorra indevida violação à propriedade intelectual em nome de uma possível ampliação dos direitos dos titulares dos dados.[62] Inferências e dados derivados tendem a depender do labor do controlador e muitas vezes são parte integrante do seu modelo de negócios. Por exemplo, o modo como se obtém um escore de crédito para uma análise de um financiamento depende muitas vezes de modelos estatísticos, pesos e critérios que podem ser específicos da visão empresarial de cada empresa. Em outras situações, pode haver o uso de algoritmos proprietários ou técnicas de inteligência artificial para se chegar ao dado inferido. Deste modo, há que se ter cuidado sobre como deve ocorrer a portabilidade.

Em uma estrutura aberta como se propõe ser o *open banking*, será crucial as determinações dos corpos técnicos para ter claro quais campos (de dados) podem ou não ser portados. Nesse sentido, deve haver uma interação clara entre os diferentes órgãos regulatórios (veja mais abaixo) e os atores do sistema. Uma participação multisetorial tende a proporcionar uma possibilidade maior de acerto e de compatibilidade entre as obrigações, interesses e necessidades de todos os agentes (inclusive dos titulares de dados).

Outro ponto que poderá gerar conflitos na aplicação do direito à portabilidade é a possibilidade de o exercício desse direito envolver informações de terceiro. Poderia o titular realizar a portabilidade dos registros de suas atividades bancárias mesmo que contenham dados pessoais de terceiro, com quem eventualmente realizou alguma transação financeira (transferência, depósito, pagamento etc)?

Ainda que possa existir alguma controvérsia, aparentemente a resposta mais compatível é afirmativa. Nesses casos, socorrendo-se ao entendimento que vem sendo adotado na interpretação do regulamento europeu sobre proteção de dados,[63] é admissível que em situações excepcionais haja a transmissão de dados pessoais de terceiro, desde que a informação desse terceiro esteja inevitavelmente associada ao dado pessoal do titular exercente do direito à portabilidade e, ainda, que sejam adotadas medidas que restrinjam os tratamentos que poderão ser feitos pelo novo controlador com os dados pessoais do terceiro.

A Autoridade do Reino Unido para a proteção de dados (*Information Commissioner's Office – ICO),* alinhada às diretrizes[64] do Grupo de Trabalho do Artigo 29,[65] apresenta o seguinte esclarecimento a respeito da inclusão de dados pessoais de terceiro no exercício do direito à portabilidade:

> *Generally speaking, providing third party data to the individual making the portability request should not be a problem, assuming that the requestor provided this data to you within their information in the first place. However, you should always consider whether there will be an adverse effect on the rights and freedoms of third parties, in particular when you are transmitting data directly to another controller.*[66]

Considerando, entretanto, a potencial controvérsia sobre esses aspectos relacionadas ao direito à portabilidade, há de se aguardar as orientações da Autoridade Nacional de Proteção de Dados Pessoais para que se tenha maior segurança jurídica acerca dos parâmetros que deverão ser observados no exercício desse direito. Relevante também será a regulamentação técnica que os grupos de trabalho de *open banking* prestarão. Esses sim estabelecerão os campos específicos que poderão ser portados e apresentarão os padrões a serem adotados.

Contudo, deve-se diferenciar a portabilidade do "uso compartilhado de dados". Se a primeira é um direito a ser exercido consoante a vontade do titular dos dados, o segundo pode ocorrer mesmo sem o consentimento de seu titular, caso os controladores possuam uma base legal para tanto. No caso do *open banking*, apesar de ter-se definido que o consentimento será a base legal aplicável para que seja autorizado o compartilhamento dos dados entre as distintas instituições financeiras e provedores de serviços de meios de pagamento,[67] essa não se confunde com a portabilidade, já que não há uma "transferência" dos dados do titular para outro prestador de serviços, mas um compartilhamento entre todos os atores, autorizado pelo titular.[68]

6. RESPONSABILIDADES

Um dos pontos mais controversos relacionados ao sistema de *open banking* está na responsabilidade dos diferentes atores pela proteção e segurança de dados que devem ser circular no sistema (tornados disponíveis). Por um lado, há a responsabilidade regulatória pela proteção de dados que o controlador original dos dados deve ter. Por outra, está a responsabilidade pela obtenção do consentimento do titular que resta com quem requer os dados. E ao redor de ambos está a responsabilidade pelos potenciais incidentes de segurança – perda, acesso não autorizado, modificação, entre outros.

A Resolução Conjunta nº 01/2020, em consonância com os pilares da segurança da informação, determina que as instituições participantes são responsáveis pela confiabilidade, integridade, disponibilidade, segurança e sigilo dos dados compartilhados. A norma, no entanto, não individualiza as respectivas responsabilidade dos atores da cadeia de fornecimento – o que cada um deve se responsabilizar por.

Do ponto de vista do titular de dados, poder-se-ia entender que todos os atores do sistema são solidariamente responsáveis pelo bom funcionamento e pela confiabilidade dos compartilhamentos. O Art. 31 da resolução preconiza que as regras da legislação em vigor, como o Código de Defesa do Consumidor e da LGPD, deverão ser observadas, naquilo em que forem aplicáveis. *In verbis:*

> *a instituição participante é responsável pela confiabilidade, pela integridade, pela disponibilidade, pela segurança e pelo sigilo em relação ao compartilhamento de dados e serviços em que esteja envolvida, bem como pelo cumprimento da legislação e da regulamentação em vigor.*[69]

Em outras palavras, não criou normas específicas de responsabilidade para o *open banking*. Essa regra sugere que a instituição transmitente será, a princípio, a responsável pela qualidade dos dados compartilhados e, a partir do compartilhamento, essa responsabilidade passará a ser repartida com a instituição receptora, especialmente quanto ao dever de conferir segurança e manter em sigilo as informações. Todavia, perante ao titular dos dados, enquanto consumidor, qualquer das instituições participantes poderá vir a ser responsabilizada pelos danos que ele sofrer, independentemente de sua efetiva contribuição; pois restaria atraída a incidência da responsabilização objetiva prevista no Código de Defesa do Consumidor. Isso claro, sempre que haja uma relação de causalidade entre o dano e a participação no sistema de *open banking*.

Sobre o ponto, importante levar em conta o teor da súmula 479 do Superior Tribunal de Justiça em que se estabelece que “as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno

relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias".

O titular de dados também estará amparado pelas regras de proteção de dados (LGPD, por exemplo) que criam obrigações do controlador para com o titular. Nesse contexto, há uma circunstância pontual em que na medida que os atores do sistema (participantes do *open banking*) tornam-se controladores dos dados, tornam-se também responsáveis pela sua proteção e na observância dos direitos dos titulares.

Como se pode verificar, a análise da responsabilidade das instituições participantes do *open banking* sob a orientação da LGPD não é tarefa simples. Para individualizar as responsabilidades sob as regras dos artigos 42 a 45 da LGPD, torna-se imprescindível que se faça apreciações casuísticas, a fim de delimitar os papéis exercidos (p. ex. controlador, operador, co-controlador).

Só conhecendo os detalhes da operação de tratamento de dados será possível entender o papel de cada agente envolvido e, assim, particularizar a sua responsabilidade. Precisará ser compreendida a operacionalização do sistema para verificar até que ponto a instituição que transmite os dados atuará como controladora da operação de tratamento de dados e partir de quando a receptora dos dados assumirá esse papel.

Nesse sentido, é prudente que se aguarde a celebração da convenção a que alude o art. 44 da Resolução Conjunta nº 01/2020 (chamada de autorregulação assistida), pois ela definirá os padrões tecnológicos e os procedimentos operacionais do sistema, permitindo que se perceba com maior nitidez a divisão de responsabilidades entre os participantes do *open banking* no que concerne às obrigações sobre proteção de dados.

Com efeito, para afastar o risco de as instituições participantes arcarem uma responsabilidade solidária e ilimitada, melhor que sejam estabelecidas balizas claras e objetivas acerca da demarcação de responsabilidades no uso do *open banking*.

7. DESAFIOS À REGULAÇÃO

Embora se vislumbre aderência da regulamentação do *open banking* com as regras sobre proteção de dados estabelecidas LGPD, isso não quer dizer que não existam desafios regulatórios pela frente.

Já se percebe que o *open banking* envolve questões relacionadas ao direito da concorrência, à proteção de dados pessoais e ao sistema financeiro nacional, o que atrai a necessidade de a matéria ser analisada e regulamentada sob enfoques distintos.

Com efeito, a regulamentação do *open banking* impõe a difícil tarefa de conciliar regras que sejam adequadas para atender todas essas suas múltiplas finalidades, que se encontram submetidas às competências regulatórias de entes distintos.

Considerando, porém, a ideia anteriormente explicada quanto à centralidade da proteção de dados pessoais no sistema, parece-nos que a LGPD traz o norte que deverá guiar as autoridades reguladoras nesse enorme desafio.

Tendo em perspectiva a primazia da proteção de dados e o que estabelecem os artigos 55-J, XXIII[70] e 55-K, parágrafo único[71] da LGPD, pensamos que deverá incumbir à Autoridade Nacional de Proteção de Dados Pessoais o papel de se articular com o CADE, o Conselho Monetário Nacional e o Banco Central do Brasil para complementar o regulamento existente, especialmente para que o *open banking* esteja em harmonia com as regras (legais e regulatórias) sobre proteção de dados pessoais.

Há, como visto neste relatório, questões complexas (como, por exemplo, a responsabilidade das instituições participantes) que precisam estar mais claramente disciplinadas.

A regulamentação inicial do *open banking* foi um avanço indiscutível, o que não afasta a necessidade de adequações para que sejam efetivamente atendidas todas as suas múltiplas finalidades (concorrencial, proteção de dados, aprimoramento do mercado bancário etc). Isso exigirá uma atuação concertada dos órgãos reguladores para, respeitadas as suas respectivas competências, avançar na elaboração de regras claras, capazes de conferir segurança jurídica nas questões mais controversas. Sem esquecer a participação dos diferentes atores do sistema em uma ação multisetorial.

8. CONCLUSÃO

O *open banking* suscita oportunidades promissoras, ainda que existam desafios a serem tomados em consideração. A possibilidade de criar um sistema aberto em que diferentes atores do sistema financeiro podem participar traz um mundo de opções. A centralidade na portabilidade de dados que o sistema brasileiro instituiu é um grande passo inicial. Em uma lógica em que exista interoperabilidade de sistemas e que se possa utilizar de maneira mais aberta e livre os diferentes serviços disponíveis no mercado, o sistema financeiro no Brasil pode se transformar, expandir, inovar e criar soluções que incluam a parcela significativa da população que ainda não tem acesso a esses serviços.

É certo que serão necessários ajustes para viabilizar o pleno funcionamento desse sistema financeiro aberto e para que sejam alcançados os seus múltiplos objetivos, assim como encontrar o padrão que garanta um nível alto de autodeterminação informativa. Há que se ter em mente que a

portabilidade de dados deve ser tomada a sério, com os devidos cuidados e considerações. Sendo a portabilidade das transações e a interoperabilidade das múltiplas áreas do setor financeiro, o próximo passo

O êxito desse processo, dadas as características do *open banking*, dependerá da atuação concertada dos órgãos reguladores e dos agentes regulados, que precisarão estar genuinamente imbuídos no propósito de superar as dificuldades e levar adiante a implementação dessa poderosa ferramenta de inovação. Um dos elementos cruciais é a relação de segurança que todos os atores devem ter entre si. E há um espaço de responsabilidade para cada um deles e particularmente para os entes da administração pública que estão por trás da implementação e manutenção da infraestrutura técnica e regulatória.

Nesse primeiro relatório é possível encontrar breves reflexões elementares sobre esse tema e alguns dos seus aspectos mais complexos, analisados sob a ótica da proteção de dados. Entende-se aqui que há uma importante confluência entre expandir o mercado financeiro, liberar as forças de inovação, permitir mais atores no sistema e ao mesmo tempo atingir os objetivos de proteção de dados e interoperabilidade de sistemas. Em um segundo relatório iremos focar precisamente nos ganhos, desafios e riscos da interoperabilidade e da portabilidade de dados para o sistema financeiro aberto (*open banking)*.

NOTAS

1. “A combinação entre objetos inteligentes e Big Data poderá alterar significativamente a maneira como vivemos. Algumas pesquisas estimam que em 2020 a quantidade de objetos interconectados passará dos 25 bilhões, podendo chegar a 50 bilhões de dispositivos inteligentes.” (Entre dados e robôs: ética e privacidade na era da hiperconectividade / Eduardo Magrani. — 2. ed. — Porto Alegre: Arquipélago Editorial, 2019)

2. Ibid.

3. World Bank, The Bali Fintech Agenda: A Blueprint for Successfully Harnessing Fintech’s Opportunities,2018. Disponível em:

https://www.worldbank.org/en/news/press-release/2018/10/11/bali-fintech-agenda-a-blueprint-for-successfully-harnessing-fintechs-opportunities

4. PWC, A nova fronteira do crédito no Brasil, 2019. Disponível em: https://www.pwc.com.br/pt/estudos/setores-atividades/financeiro/2019/pesquisa-credito-digital-19.pdf.

5. PWC, Opening the bank for a new era of growth, 2018. Disponível em: https://www.pwc.com/us/en/financial-services/publications/assets/pwc-fs-digital-open-banking.pdf.

6. Fintech Radar. Disponível em: https://www.finnovista.com/en/radar/brasil-recupera-el-liderazgo-fintech-en-america-latina-y-supera-la-barrera-de-las-370-startups/.

7. Banco Central do Brasil, Relatório de Economia bancária, 2019. Disponível em: https://www.bcb.gov.br/content/publicacoes/relatorioeconomiabancaria/REB_2019.pdf.

8. As instituições que compõem esses dois grupos são: S1 - bancos múltiplos, comerciais, de investimento, de câmbio, além de caixas econômicas cujo porte seja igual ou superior a 10% do PIB nacional - o exercício de atividade internacional significativa também qualifica para esse grupo; S2 - de investimento, de câmbio, além de caixas econômicas cujo porte seja esteja entre 1 e 10% do PIB. .

9. Disponível em: https://www.in.gov.br/en/web/dou/-/comunicado-nº-33.455-de-24-de-abril-de-2019-85378506.

10. Art. 2º, inciso I, da Resolução Conjunta nº 01/2020.

11. Art. 3º da Resolução Conjunta nº 01/2020.

12. Trecho de notícia veiculada pelo Banco Central do Brasil para informar sobre o início do processo de implementação do open banking. Disponível em https://www.bcb.gov.br/detalhenoticia/16733/nota.

13. Os gastos globais voltados à privacidade em ferramentas de conformidade alcançarão US$ 8 bilhões até 2020: https://inforchannel.com.br/gartner-em-tres-anos-mais-de-40-da-tecnologia-para-privacidade-dependera-de-ia/.

14. Disponível em: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

15. Disponível em https://publications.iadb.org/en/fintech-latin-america-2018-growth-and-consolidation.

16. Disponível em https://www.bcb.gov.br/content/publicacoes/relatorioeconomiabancaria/REB_2019.pdf.

17. GOETTENAUER, Carlos. Open Banking e o Modelo de Banco em Plataforma: a necessidade de reavaliação da definição jurídica de atividade bancária. Revista da Procuradoria-Geral do Banco Central, [S.l.], v. 14, n. 1, p. 13-27, set. 2020. ISSN 1982-9965. Disponível em https://revistapgbc.bcb.gov.br/index.php/revista/article/view/1025

18. BARBERIS, J. N.; BUCKLEY, R. P.; ARNER, D. W. The Evolution of Fintech: A New Post-Crisis Paradigm? University of Hong Kong Faculty of Law Research Paper No. 2015/047, 20 out. 2015. Disponivel em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2676553.

19. BARBERIS, J. N.; BUCKLEY, R. P.; ARNER, D. W. FinTech, RegTech, and the Reconceptualization of Financial Regulation. Northwestern Journal of International Law & Business, v. 37, n. 3, 2017.

20. MAGNUSON, W. J. Regulating Fintech. In.: Vaderbilt Law Review, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3027525.

21. Organizações de caráter internacional como o Fundo Monetário Internacional e o Banco Interamericano de Desenvolvimento vêm como um setor em franca expansão e que vai muito além de meios de pagamento. Veja por exemplo: IDB/Finnovisa, Report on Fintech in Latin America 2018: Growth and Consolidation. Disponível em: https://publications.iadb.org/publications/english/document/Fintech-Latin-America-2018-Growth-and-Consolidation-final.pdf; IMF, Fintech: The Experience so Far, June, 2019. Disponível em: https://www.imf.org/en/Publications/Policy-Papers/Issues/2019/06/27/Fintech-The-Experience-So-Far-47056.

22. “(...) não há como deixar de reconhecer que o livre trânsito dos dados pessoais estimula a concorrência e, portanto, possibilita o direito de escolha do consumidor, tutelando de forma inegável o bem-estar desses. Trata-se da tutela do consumidor manejada por meio do direito da concorrência, reforçando e dando aplicabilidade aos princípios da Ordem Econômica, nomeadamente ao princípio da livre concorrência (art. 170, inciso IV, da CF) e da defesa do consumidor (art. 170, inciso V, da CF).” (CRAVO, Daniela Copetti. O direito à portabilidade na Lei de Proteção de Dados. In: Ana Frazão; Gustavo Tepedino; Milena Donato Oliva. (Org.). Lei Geral de Proteção

de Dados Pessoais e suas repercussões no Direito Brasileiro. 1ed.São Paulo: Revista dos Tribunais, 2019, v. 1, p. 347-366)

23. Ainda que se tenha em mente originalmente novos atores, como startups, deve-se notar que há uma série de iniciativas de instituições mais tradicionais que seguem nesse mesmo caminho de experimentação adaptação rápida às transformações digitais. Veja nesse sentido: IMF, Fintech: The Experience so Far, June, 2019. Disponível em: https://www.imf.org/en/Publications/Policy-Papers/Issues/2019/06/27/Fintech-The-Experience-So-Far-47056.

24. "(...) há uma grande aposta que a General Data Protection Regulation e a Lei Geral de Proteção de Dados Pessoais (Lei n.13.709/2018) tragam efeitos concretos para o debate concorrencial. Primeiro, porque entre os novos "direitos digitais" garantidos pelas leis de proteção de dados pessoais está o direito à portabilidade de dados pessoais (presente no rol do art. 18, Lei n.13.709/2018)." ZANATTA, R. A. F.; ABRAMOVAY, R. Dados, vícios e concorrência: repensando o jogo das economias digitais. Estud. av., São Paulo, v. 33, n. 96, p. 421-446, Aug. 2019. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-40142019000200421&lng=en&nrm=iso.

25. Telesintese, Open Banking vai estimular o surgimento de mais de 700 fintechs no Brasil, prevê ABFINTECHS - Disponível em https://www.telesintese.com.br/open-bank-vai-estimular-o-surgimento-de-mais-700-fintechs-no-brasil-preve-abfintechs/.

26. Open Banking: impactos sobre a concorrência e o bem-estar do consumidor. Disponível em https://www.conjur.com.br/2020-jul-11/opiniao-impacto-open-banking-concorrencia-consumidor.

27. Ibid.

28. Disponível em: https://inforchannel.com.br/gartner-em-tres-anos-mais-de-40-da-tecnologia-para-privacidade-dependera-de-ia/

29. Segundo o relatório da Gartner, atualmente, a Inteligência Artificial representa apenas 5% da tecnologia voltada para a conformidade com as leis de privacidade, mas a previsão é de que esse número aumente para 40% até 2023. Ibid.

30. "O Open Banking, na ótica do Banco Central do Brasil, é considerado o compartilhamento de dados, produtos e serviços pelas instituições financeiras e demais instituições autorizadas, a critério de seus clientes, em se tratando de dados a eles relacionados, por meio de abertura e integração de plataformas e infraestruturas de sistemas de informação, de forma segura, ágil e conveniente." (Trecho do Comunicado nº 33.455/2019. Disponível em https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Comunicado&numero=33455).

31. Ainda que a visão seja inclusiva, a lógica é que as grandes instituições sejam obrigadas e as menores tenham a oportunidade de se juntar (assim como mencionado acima). Interessante notar que no caso da infraestrutura de pagamentos instantâneos PIX, a obrigatoriedade foi no sentido não necessariamente do porte mas sim do número de contas 500 mil ativas.

32. "At a very basic level, an application programming interface, or API, is "a way for two computer applications to talk to each other over a network using a common language that they both understand" (Jacobson et al., 2012). Editor-in-Chief of ProgrammableWeb.com, David Berlind describes APIs as "electrical sockets that have predictable patterns of openings"1 into which, other applications that match those patterns can "plug in" and consume them in the same way electrical devices consume electricity." (Zachariadis, Markos and 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.

33. Artigos 23 e seguintes da Resolução Conjunta nº 01/2020.

34. "Committee members have identified a variety of potential operational and cyber security issues related to the use of APIs, including data breaches, misuse, falsification, denial of service attacks and unencrypted login. Other types of identified risks include infrastructure malfunction, speed of execution and operations, man-in-the-middle attack, token compromise and IP address spoofing. An API gateway could also be a single point of failure if not designed to be resilient. Mechanisms used by some banks to mitigate these risks include stricter access privileges, authorised end-to-end encryption, authentication mechanisms, vulnerability testing, establishing an audit trail, setting expiration times for tokens, IP whitelisting, firewalls and monitoring cyber incidents related to APIs as part of the overall cyber incident monitoring program." (Report on open banking and application programming interfaces. Novembro de 2019. Bank for International Settlements. Disponível em https://www.bis.org/bcbs/publ/d486.pdf).

35. Segundo notícia divulgada pelo Senado Federal, o Brasil é o 2º país no mundo em perdas por ataques cibernéticos. Disponível em https://www12.senado.leg.br/noticias/materias/2019/09/05/brasil-e-2o-no-mundo-em-perdas-por-ataques-ciberneticos-aponta-audiencia.

36. Art. 4º As instituições de que trata o art. 1º, para fins do cumprimento dos objetivos de que trata o art. 3º, devem conduzir suas atividades com ética e responsabilidade, com observância da legislação e regulamentação em vigor, bem como dos seguintes princípios: (...)

II - segurança e privacidade de dados e de informações sobre serviços compartilhados no âmbito desta Resolução Conjunta;

37. Art. 8º A solicitação de compartilhamento de dados de cadastro e de transações e de serviços de que trata o art. 5º, incisos I, alíneas "c" e "d", e inciso II, alínea "a", compreende as etapas do consentimento, autenticação e confirmação.

Parágrafo único. As etapas de que trata o caput devem:

I - ser efetuadas com segurança, agilidade, precisão e conveniência, por meio da interface dedicada de que trata o art. 23;

38. Art. 18. Os procedimentos e controles para autenticação de que tratam os arts. 16 e 17 devem ser compatíveis com a política de segurança cibernética da instituição, prevista na regulamentação em vigor.

39. Art. 31. A instituição participante é responsável pela confiabilidade, pela integridade, pela disponibilidade, pela segurança e pelo sigilo em relação ao compartilhamento de dados e serviços em que esteja envolvida, bem como pelo cumprimento da legislação e da regulamentação em vigor.

40. Art. 33. O diretor responsável pelo compartilhamento de que trata o art. 32 deve elaborar relatório semestral referente ao compartilhamento de dados e serviços em que a instituição esteve envolvida, nas datas-bases de 30 de junho e 31 de dezembro.

§ 1º O relatório de que trata o caput deve abordar, no mínimo: (...)

III - os incidentes relacionados com a violação da segurança dos dados e informações sobre serviços relacionados ao compartilhamento, bem como as medidas adotadas para a sua prevenção e solução de que tratam os arts. 38, § 3º, e 48, inciso III, se for o caso;

41. Art. 38. O contrato de que trata o art. 36 deve prever, no mínimo: (...)

IV - a adoção de medidas de segurança para a recepção e o armazenamento pelo parceiro contratado dos dados ou informações sobre serviços compartilhados de clientes; (...)

§ 3º A obrigação de que trata o inciso X do caput deve contemplar a comunicação de incidentes de violação da segurança dos dados e informações sobre serviços relacionados ao compartilhamento e as medidas adotadas pelo parceiro contratado para a sua prevenção e solução.

42. Art. 39. A instituição contratante é responsável pela confiabilidade, pela disponibilidade, pela segurança e pelo sigilo do compartilhamento de que trata o art. 36, bem como pelo cumprimento da legislação e da regulamentação em vigor.

43. 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: (...)

§ 2º Os mecanismos de que trata o caput devem: (...)

II - ser compatíveis com a política de segurança cibernética da instituição, prevista na regulamentação em vigor; e

44. Art. 44. As instituições participantes devem celebrar convenção, com observância das disposições desta Resolução Conjunta, sobre aspectos relativos:

I - aos padrões tecnológicos e aos procedimentos operacionais, que abrangem, no mínimo:

a) a implementação de interfaces dedicadas de que trata o art. 23, inclusive: (...)

4. os controles de acesso às interfaces e aos dados; (...)

b) os padrões e certificados de segurança; e

45. Art. 48. As instituições devem assegurar que suas políticas para gerenciamento de riscos, previstas na regulamentação em vigor, disponham, com relação à continuidade de negócios, sobre: (...)

III - o tratamento de incidentes relacionados com a violação da segurança dos dados relacionados ao compartilhamento e as medidas tomadas para a sua prevenção e solução; e

46. Há aqui uma distinção importante no sentido de que open banking é mais amplo do que a interoperabilidade dos sistemas de meios de pagamento. para fazer uma analogia, o sistema PIX é um sistema que facilita a interoperabilidade dos meios de pagamento, mas é uma parte do todo que é o sistema financeiro aberto.

47. "A interoperabilidade técnica é condição essencial da concorrência. A fim de criar um mercado integrado dos sistemas de pagamento eletrônico em euros, é indispensável que o processamento das transferências a crédito e dos débitos diretos não seja entravado por regras de negócio ou por obstáculos técnicos, tais como a adesão obrigatória a mais de um sistema de liquidação de pagamentos transfronteiriços. As transferências a crédito e os débitos diretos deverão ser efetuados ao abrigo de um modelo cujas regras de base tenham a adesão de PSP que representem a maioria dos PSP da maioria dos Estados-Membros e constituam a maioria dos PSP da União e que sejam as mesmas para as operações de transferência a crédito e de débito direto tanto transfronteiriças como puramente nacionais. Se existir mais de um sistema de pagamento para o processamento destes pagamentos, tais sistemas deverão ser interoperáveis mediante a utilização de normas à escala da União e de normas internacionais, de modo a que todos os PSU e PSP possam beneficiar de pagamentos de retalho em euros sem descontinuidades em toda a União." (Considerando nº 10 do Regulamento (UE) nº 260/2012)

48. “In more recent years, however, a new type of entity has developed: third party payment providers. These actors allow consumers to, for instance, make online payments without the need for a credit card by establishing a “link between the payer and the online merchant via the payer’s online banking module”.3 A number of third party payment providers have become very successful within the EU, important examples being SOFORT in Germany, iDEAL in the Netherlands and Trustly in Sweden. These third party payment providers do not require the consumer to open an account directly with them. Instead, they gather information on the consumer’s existing bank accounts and present that information in an integrated manner.” (Valcke, Peggy and Vandezande, Niels and Van de Velde, Nathan, The Evolution of Third Party Payment Providers and Cryptocurrencies Under the EU’s Upcoming PSD2 and AMLD4 (September 23, 2015). SWIFT Institute Working Paper No. 2015-001) Disponível em https://ssrn.com/abstract=2665973.

49. À época da adoção desses instrumentos normativos pela União Europeia o Reino Unido era um de seus Estados-Membros, situação que persistiu até 1º de fevereiro de 2020 quando se confirmou o Brexit.

50. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/544942/overview-of-the-banking-retail-market.pdf.

51. “We are putting in place a wide range of measures to provide a coherent package that will target the problems we have identified. Many of our remedies build on those introduced by past reviews and on recent positive developments. But we are now in a position to significantly accelerate the pace of change by harnessing technology. In particular, we are requiring banks to allow their customers to share their own bank data securely with third parties using an open banking standard. This change, together with our other remedies, will help customers to find and access better value services and enable them to take more control of their finances. This will also enable new entrants and smaller providers to compete on a more level playing field and increase the opportunities for new business models to develop.” Idem.

52. Veja as definições propostas pela corporação no Reino Unido: https://www.openbanking.org.uk/customers/what-is-open-banking/.

53. Disponível em: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202006_interplaypsd2andgdpr.pdf.

54. Disponível em: https://www.bcb.gov.br/pre/normativos/busca/downloadVoto.asp?arquivo=/Votos/CMN/202044/Voto%200442020_CMN.pdf.

55. Art. 2º, inciso VIII, da Resolução Conjunta nº 01/2020.

56. Art. 10 da Resolução Conjunta nº 01/2020.

57. Artigo 18 da LGPD.

58. A Convenção de que trata o art. 44 da Resolução Conjunta nº 01/2020 deve prescrever esses mecanismos e o meio como as interfaces devem ser desenvolvidas.

59. Arts. 15 e 28 da Resolução Conjunta nº 01/2020.

60. Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: (...)

V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial.

61. “Em contrapartida, os dados inferidos e os dados derivados são criados pelo responsável pelo tratamento com base nos dados «fornecidos pelo titular dos dados». Por exemplo, o resultado de uma avaliação da saúde de um utilizador ou o perfil criado no âmbito das regulamentações de gestão dos riscos e do setor financeiro (p. ex., para atribuir uma pontuação de crédito ou cumprir regras de combate ao branqueamento de capitais) não podem, em si, ser considerados dados «fornecidos pelo» titular dos dados. Ainda que esses dados possam fazer parte de um perfil conservado por um responsável pelo tratamento e sejam inferidos ou derivados de uma análise dos dados fornecidos pelo titular dos dados (p. ex., através das suas ações), regra geral, estes dados não serão considerados «fornecidos pelo titular dos dados» e, por conseguinte, não serão abrangidos pelo âmbito deste novo direito.” (trecho das Orientações do Grupo do Artigo 29 sobre o direito à portabilidade dos dados). Disponível em https://www.cnpd.pt/home/rgpd/docs/wp242rev01_pt.pdf.

62. O antigo WP 29, hoje EDPB faz uma distinção entre dados entregues pelo titular ou observados e dados “derivados” ou “inferidos”. Estabelece que pode haver nuances no tratamento desses dados devido ao fato de que há um labor por parte do controlador para chegar a esses dados. Ainda que eles não percam o status de dados pessoais. (Art. 29 Data Port. Working Party, supra note 17, at 8; Article 29 Data Prot. Working Party, Guidelines on the Right to Data Portability, 16/EN, WP242rev.01, at 9–11, 2016, Dsiponível em: https://ec.europa.eu/newsroom/document.cfm?doc_id=44099).

63. “Infine, il WP 29 osserva che i dati di cui si tratta, oggeto di portabilità, devono essere dati relativi all’interessato e dal medesimo forniti consapevolmente e attivamente, dove infatti il paragrafo 4 dell’art. 20 GDPR prescrive che l’esercizio dela portabilità non leda i diritti e la libertà altrui. Ecco perchè il WP29 si preoccupa di chiarire che, se l’interessato richiede la transmissione di dati, laddove questi dati contengano anche informazioni relative ad altri interessati, il titolare dovrà individuare um’altra base giuridica per eseguire il tratamento sottostante l’esercizio del diritto di portabilità. Questo significa che egli non potrà trasmettere i dati giustificando

il trattamento di transmissione con l'esercizio dela portabilità da parte dell'interessato richiedente, ma dovrà comunicare che trasmette i dati, ad esempio, perchè è tenuto a fare ciò in esecuzione di um suo legittimo interesse (art. 6, (1), lett. f) GDPR). Inoltre, sottolinea WP29, in caso de transmissione di dati di terzi, il titolare ricevente dovrà trattare questi dati solamente per la finalità per cui li trattava il titolare transmittente: in caso contrario, il trattamento è illecito". (TOSSATTI, Caterina, In Privacy e Data Protection, Guida al Regolamento (EU) 2016/679 per imprese, professionisti, PA e Responsabili dela Protezione Dati (DPO). 2018. Dei Giuridica. P. 98/99).

64. "In many circumstances, data controllers will process information that contains the personal data of several data subjects. Where this is the case, data controllers should not take an overly restrictive interpretation of the sentence "personal data concerning the data subject". As an example, telephone, interpersonal messaging or VoIP records may include (in the subscriber's account history) details of third parties involved in incoming and outgoing calls. Although records will therefore contain personal data concerning multiple people, subscribers should be able to have these records provided to them in response to data portability requests, because the records are (also) concerning the data subject. However, where such records are then transmitted to a new data controller, this new data controller should not process them for any purpose which would adversely affect the rights and freedoms of the third-parties". Disponível em https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.

65. Grupo de Trabalho instituído com base no artigo 29.º da Diretiva 95/46/CE, que se constituiu em um órgão consultivo europeu independente em matéria de proteção de dados e privacidade.

66. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/

67. Nesse sentido é a Resolução Conjunta nº 01/2020 do Conselho Monetário Nacional e do Banco Central do Brasil.

68. Para uma análise mais detalhada sobre o direito à portabilidade ver VIOLA, Mario; HERINGER, Leonardo. A Portabilidade na Lei Geral de Proteção de Dados. Instituto de Tecnologia e Sociedade, 2020. Disponível em https://itsrio.org/wp-content/uploads/2020/10/A-Portabilidade-na-LGPD.pdf.

69. Art. 31 da Resolução Conjunta nº 01/2020.

70. 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.

71. Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública.

SOBRE OS AUTORES

Mario Viola
Doutor em Direito pelo Instituto Universitário Europeu (Florença, Itália), Mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro. É atualmente Pesquisador Associado do *Centre for Media Pluralism and Media Freedom* do Instituto Universitário Europeu e Consultor do Instituto de Tecnologia e Sociedade do Rio de Janeiro para os temas da privacidade e proteção de dados pessoais.

Leonardo Heringer
Advogado, sócio do escritório Borges & Schumacher Advogados

Janaina Costa
Mestre em Desenvolvimento Econômico e Social pelo IEDES - Paris 1 Panthéon-Sorbonne; Bacharel em Direito pela Universidade Federal de Minas Gerais. Pesquisadora da área de Direito e Tecnologia no Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio).

Celina Bottino
Mestre em direitos humanos pela Universidade de Harvard. Foi pesquisadora da Human Rights Watch em Nova York. Supervisora da Clínica de Direitos Humanos da FGV Direito-Rio. Foi consultora da Clínica de Direitos Humanos de Harvard e pesquisadora do ISER. Diretora de projetos do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio).

Christian Perrone
Pesquisador Fulbright (Universidade de Georgetown, EUA). Doutorando em Direito Internacional (UERJ); Mestre em Direito Internacional (L.L.M/Universidade de Cambridge, Reino Unido). Ex-Secretário da Comissão Jurídica Interamericana da OEA. Coordenador da área de Direito e Tecnologia no Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio).

Esse relatório contou com o generoso
apoio financeiro do Reino Unido através
de programa *Digital Access*

GREAT *for* PARTNERSHIP
BRITAIN & NORTHERN IRELAND

Acesse nossas redes

itsrio.org