COMENTÁRIOS DA BRASSCOM AO EDITAL DE CONSULTA PÚBLICA Nº 73/2019 – OPEN BANKING

SÃO PAULO, JANEIRO DE 2020

A Brasscom, Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação (TIC), entidade que congrega empresas fornecedoras de *software*, aplicações de *Internet*, soluções e serviços de TIC e que tem como missão trabalhar em prol do desenvolvimento do setor, disseminando seu alcance e potencializando seus efeitos sobre a economia e o bem-estar social, parabeniza a Diretoria Colegiada do Banco Central do Brasil por submeter à consulta pública propostas de circular e de resolução que tratam da implementação do Sistema Financeiro Aberto (***Open Banking***) por parte de instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central ("BACEN").

Com intuito de enriquecer o debate e contribuir para que a implementação do sistema de *Open Banking* a ser implementado no Brasil seja feita de forma robusta e que todos os seus potenciais benefícios sejam de fato auferidos, a Brasscom respeitosamente apresenta seus comentários.

1. Escopo da Resolução - Participação direta de terceiros no Sistema Financeiro Aberto

Inicialmente, a participação no ecossistema de *Open Banking* será restrita a entes integrantes do Sistema Financeiro Nacional, os quais são diretamente regulados pelo Banco Central do Brasil. Não obstante, para que a proposta atinja seu objetivo de forma eficiente, prevê-se a possibilidade de contratação de terceiros para disponibilizar aos clientes das instituições partícipes os serviços de compartilhamento dos dados e serviços de iniciação de transação de pagamento, bem como de compartilhamento de outros dados e serviços que venham a ser incluídos no escopo do sistema.

Na medida em que o ecossistema de *Open Banking* permitirá a criação de novos modelos de negócio e soluções financeiras inovadoras e considerando a essência do *Open Banking* em aumentar a concorrência através da ampliação do número de participantes do mercado com acesso aos dados de transações financeiras do consumidor, a Brasscom gostaria de sugerir ao BACEN a ampliação do escopo da Resolução, permitindo que outros *players* possam aproveitar e contribuir com esse ecossistema emergente.

O *Open Banking* tem sido legislado em alguns países do mundo e, nesse sentido, é relevante destacar a experiência internacional sobre este tema.

1.1. União Europeia

A UE regulamenta a partilha de dados da conta bancária dos consumidores com prestadores de serviços de pagamento de terceiros através da Diretiva de Serviços de

Pagamento revista (PSD2)[1], o qual entrou em vigor em setembro de 2019. Sob essa normativa, são contempladas 3 figuras regulatórias:

- Prestador de serviços de pagamento que gere a conta (ASPSP): um prestador de serviços de pagamento que disponibiliza e mantém contas de pagamento para um cliente/ordenante (bancos tradicionais e instituições de pagamento);
- Prestador do serviço de iniciação do pagamento (PISP): oferece o serviço de iniciação de uma ordem de pagamento a pedido do utilizador do serviço de pagamento relativamente a uma conta de pagamento detida noutro prestador de serviços de pagamento (empresas que atuariam como meios de pagamento); e
- Prestador de serviços de informação sobre contas (AISP): oferece serviços online para prestação de informações consolidadas sobre uma ou mais contas de pagamento detidas pelo utilizador de serviços de pagamento junto a outro ou outros prestadores de serviços de pagamento.

No que diz respeito à proposta brasileira, as figuras de referência seriam apenas os ASPSP e os PISP. Esta última, juntamente com o AISP, é regulamentada como um *Third Party Provider* (TPP), que não necessariamente se caracteriza como um player do sistema financeiro. As empresas que operam como TPP estão sujeitas aos mesmos requisitos e às mesmas obrigações que as instituições de pagamento sob o escopo da PSD2, com algumas excludentes regulatórias.

O principal critério a ser obedecido para se permitir a participação de terceiros no *Open Banking* europeu é a aquisição de uma licença específica em seu país de origem e a obtenção dos denominados *passporting rights*[2] para operar em outros países anfitriões europeus. Tal obrigatoriedade permite ao órgão regulador garantir a segurança das operações efetivadas através do sistema, pois a licença concedida obedece a especificidades regulatórias atinentes ao seu "guarda-chuva" legal.

Para a prestação de serviços de iniciação de pagamento, ASPSP devem possibilitar aos PISP que se baseiem nos procedimentos de autenticação segura dos clientes personalizadas – como as credenciais de segurança – para que iniciem um pagamento específico em nome do solicitante.

Os direitos e obrigações dos PISP deverão ser proporcionais aos serviços prestados. Mais especificamente, a divisão de responsabilidade entre o prestador do serviço e os ASPSP deverá corresponder às fases operacionais que, de fato, estiverem sob seus respectivos controles.

Quando o terceiro fornecer exclusivamente os serviços de PISP, não se exige a detenção, em caráter permanente, de fundos próprios. Para esse regulado, não há necessidade de estabelecer uma relação contratual com os ASPSP para fornecimento de seus serviços.

[1] Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN

[2] Permissão para que uma empresa registrada na Área Econômica Europeia (EEA) faça negócios em qualquer outro estado do EEE sem a necessidade de autorização adicional de cada país.

1.2. Reino Unido

O regime de *Open Banking* do Reino Unido é uma resposta a um relatório[3] de 2016 da Autoridade de Concorrência e Mercados (CMA) que concluiu pela falta de concorrência entre os grandes bancos já estabelecidos, o que dificultava a consolidação de *players* menores no mercado financeiro. O regime de *Open Banking* do Reino Unido é implementado por meio da Ordem de Investigação do Mercado Bancário de Varejo 2017[4], que exige que os nove maiores bancos do Reino Unido forneçam aos provedores regulamentados acesso aos dados bancários do cliente por meio de um formulário seguro e padronizado, mediante solicitação dos clientes.

A implementação do sistema bancário aberto no Reino Unido baseia-se nas obrigações do PSD2, exigindo que os bancos forneçam dados a terceiros em um formato de API padrão. Terceiros que usam APIs publicadas para acessar dados de clientes são autorizados e regulados pela Financial *Conduct Authority* (FCA) e inscritos no *Open Banking Directory.*

Destaca-se em relação à experiência britânica a possibilidade dos denominados Prestadores de Serviços Técnicos (TSP)[5] poderem se registrar junto ao *Directory Sandbox*[6] gratuitamente para testar seus serviços tecnológicos abertos, de forma segura e com dados fictícios. As empresas interessadas em atuar sob o escopo dessa figura regulatória devem estar registradas na União Europeia. Nesse caso, é feita uma checagem de informações antes da concessão da permissão para testes; se não houver regulação prévia, são feitas algumas verificações adicionais acerca da empresa e de seus diretores – o que inclui garantir que sua empresa e seus diretores não apareçam em nenhuma lista de sanções, listas de observação ou registros de imposição. Finalizada a fase de testes, os TSP poderão usar a lista de TPP e ASPSP já regulados como referência para firmar parcerias e oferecer seus serviços.

Nesse sentido, nós entendemos ser pertinente estabelecer a relação entre o objeto da Consulta Pública 72/2019[7], que "divulga proposta de atos normativos dispondo sobre o Ambiente Controlado de Testes para Inovações Financeiras e de Pagamento (Sandbox Regulatório) e sobre as condições para o fornecimento de produtos e serviços no contexto desse ambiente e no âmbito do Sistema Financeiro Nacional e do Sistema de Pagamentos Brasileiro" com o propósito da consulta pública de *Open Banking* tendo em vista que a intenção da autoridade financeira com a proposta de Sandbox Regulatório é "permitir que instituições já autorizadas e ainda não autorizadas a funcionar pelo Banco Central do Brasil possam testar projetos inovadores (novos produtos, serviços ou modelos de negócio) com clientes reais, sujeitos a requisitos regulatórios específicos", é razoável considerar que os resultados obtidos pudessem ser incorporados ao sistema *Open Banking.*

---

[3] Disponível em: https://www.openbanking.org.uk/customers/regulated-providers/

[4] Disponível em: https://www.gov.uk/government/publications/retail-banking-market-investigation-order-2017

[5] Empresas que trabalham com provedores regulamentados para fornecer produtos ou serviços bancários abertos.

[6] Disponível em: https://directory.openbanking.org.uk/s/login/

[7] Disponível em: https://www3.bcb.gov.br/audpub/DetalharAudienciaPage?3&pk=321.

Desta forma, a participação de terceiros poderia ser oportunizada com as devidas salvaguardas regulatórias, sem, no entanto, exigir de novos possíveis players do sistema o elevado ônus de se obter uma licença integral para atuação no mercado junto ao Banco Central. Ademais, dentro das prioridades estratégicas que guiarão o Sandbox a ser regulamentado pelo BACEN, estão soluções para o Open Banking e para aumentar a concorrência no sistema de pagamentos. Nesse sentido, entendemos que o Sandbox regulatório pode ser uma boa oportunidade para novos entrantes (tais como *fintechs* e empresas de tecnologia) participarem do desenvolvimento do sistema financeiro brasileiro. Nesse contexto, seria importante, inclusive, o esclarecimento de eventuais métricas para tal atuação, a exemplo do tamanho da empresa, de participação no mercado ou de adoção por parte do usuário como credenciamento para participação desses novos entrantes no Sandbox.

2. Sistema de *Open Banking* e a Lei Geral de Proteção de Dados ("LGPD")

É inegável que a implementação do sistema de "*Open Banking*" no Brasil democratizará a oferta de produtos e serviços relacionados ao Sistema Financeiro Nacional, propiciando desenvolvimento econômico ao estimular a livre iniciativa e prestigiar a livre concorrência de atividade econômica com importância fundamental para o país.

A regulamentação do tema, no entanto, precisa se respaldar na legislação específica aplicável, assim como não pode se olvidar, no que toca à proteção de dados pessoais, da lei geral que regula a matéria, a Lei Geral de Proteção de Dados Pessoais, Lei 13.709/2018, que entrará em vigor em agosto de 2020.

O objeto da LGPD é a **proteção do dado pessoal**[8], definido como toda informação relacionada a pessoa natural identificada ou identificável. O "tratamento"[9], por sua vez, é considerado pela LGPD como toda e qualquer atividade ou operação realizada com dados pessoais.

Assim, qualquer atividade relacionada ao tratamento de dados pessoais[10], para que seja considerada regular precisa se respaldar em uma ou mais hipóteses legais autorizativas de sua utilização, conhecidas como "bases legais" da LGPD. Isso significa dizer que, segundo a LGPD, qualquer a atividade de tratamento de dados pessoais somente será considerada legal/válida se estiver justificada em, pelo menos, uma das dez hipóteses ou bases legais que permitem a utilização dos dados pessoais. Caso o tratamento de dados pessoais não se encaixe em algum dos permissivos legais da LGPD, referido tratamento será inadequado.

Desta forma, a LGPD traz como algumas das bases legais que legitimam o tratamento de dados pessoais, além do consentimento do titular dos dados pessoais, o cumprimento de obrigação legal ou regulatória, a execução de contrato, o exercício regular de direito em processos administrativo, arbitral ou judicial, o interesse legítimo daquele que utiliza os dados pessoais ou de terceiros, a proteção ao crédito, dentre outras[11].

---

[8] Art. 5º, inciso I, da Lei 13.709/2018.

[9] Art. 5º, inciso X, da Lei 13.709/2018.

[10] Ressalvadas as exceções legais previstas no Art. 4º da LGPD.

[11] A LGPD traz as bases legais de tratamento de dados pessoais em seus artigos 7º, 11 e 14. O art. 7º se refere aos dados pessoais "comuns"; o art. 11, se refere aos dados pessoais sensíveis e no art. 14, o

Importante ressaltar que, segundo a LGPD, nenhuma das bases legais tem prevalência sobre outra, elas têm o mesmo valor sem haver qualquer hierarquia entre elas.

Dito de outra forma, o tratamento de dados pessoais, pelo mandamento da LGPD, não depende necessariamente do consentimento para ocorrer. Depende da existência de uma das bases legais de tratamento previstas na lei, respeitados os princípios e demais mandamentos dessa.

E, em virtude de a LGPD estabelecer um *framework* referente à proteção de dados pessoais, ela se aplica a todo e qualquer setor que se utilize de dados pessoais em suas atividades.

Portanto, as operações sujeitas à LGPD igualmente abrangem aquelas realizadas por instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil (BACEN). Indubitavelmente a essas operações financeiras é aplicável um arcabouço legislativo específico, formado pelas leis especiais e, através de embasamento legal, pelas normas infralegais emitidas pelo Banco Central do Brasil e pelo Conselho Monetário Nacional (CMN), entidades integrantes do Sistema Financeiro Nacional[12] com poder regulamentar nas matérias que lhe são pertinentes.

---

tratamento se refere aos dados pessoais de crianças e adolescentes. Embora o consentimento exigido pela LGPD nesses dois últimos casos seja mais rigoroso, ele não é dotado de superioridade legal. V. os artigos mencionados: **Art. 7º**. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular; II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente**. 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; II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. **Art. 14.** O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente. § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

[12] V. art. 1º da Lei n. 4595/1964.

Nesse particular uma das leis especiais aplicáveis para o caso é a Lei Complementar Nacional n. 105, de 10 de janeiro de 2001, na medida em que trata de dados pessoais ao dispor sobre "o sigilo das operações de instituições financeiras". Logo em seu artigo 1º é estabelecido que as **instituições financeiras** devem conservar **sigilo** em suas operações ativas e passivas, assim como em seus serviços prestados[13], prevendo ser considerado crime[14] a quebra do sigilo fora das hipóteses previstas[15] , elencadas no parágrafo 3º do seu artigo 1º, a saber:

> *"Art. 1º As instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados. (...)*
>
> *Art. 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, 7º e 9 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."*

---

[13] Art. 1o LC 105/2001: "**As instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados. § 1o São consideradas instituições financeiras**, para os efeitos desta Lei Complementar: I – os bancos de qualquer espécie; II – distribuidoras de valores mobiliários; III – corretoras de câmbio e de valores mobiliários; IV – sociedades de crédito, financiamento e investimentos; V – sociedades de crédito imobiliário; VI – administradoras de cartões de crédito; VII – sociedades de arrendamento mercantil; VIII – administradoras de mercado de balcão organizado; IX – cooperativas de crédito; X – associações de poupança e empréstimo; XI – bolsas de valores e de mercadorias e futuros; XII – entidades de liquidação e compensação; **XIII – outras sociedades que, em razão da natureza de suas operações, assim venham a ser consideradas pelo Conselho Monetário Nacional.**" (Destacou-se)

[14] Art. 10 da LC 105/2001.

[15] Art. 1º parágrafo 3o da LC 105/2001.

Além do inciso V, que se refere ao consentimento, as demais hipóteses acima mencionadas, portanto, igualmente autorizam o compartilhamento de dados, inclusive pessoais, no âmbito do sistema financeiro.

Relevante aqui esclarecer que em nenhum momento a LC 105/2001 indica ser o consentimento do interessado um fator de legitimação hierarquicamente superior às demais hipóteses legalmente admitidas para o compartilhamento de dados. É certo que o consentimento exigido pela LC 105/2001 é qualificado como "expresso"[16], entretanto, não é mais importante do que outros fatores que igualmente permitem o compartilhamento, como, por exemplo, razões de proteção ao crédito[17] , ou que até exigem como é o caso de cumprimento de obrigação legal[18]. Fosse intenção do legislador privilegiar o consentimento, ele não o teria sido simplesmente elencado juntamente com as outras hipóteses que excepcionam a quebra do sigilo.

Daí se infere que a LC 105/2001 e a LGPD são compatíveis ao não priorizar o consentimento como base legal para o compartilhamento de dados pessoais.

Diante desse cenário, não nos parece encontrar embasamento legal sólido a proposta ora apresentada no sentido de limitar o compartilhamento dos dados pessoais a um contexto de consentimento, sendo fundamental, em virtude da harmonização do ambiente legal aplicável, que todas as premissas fixadas pela LGPD sejam observadas.

3. Do Escopo do *Open Banking* e dos Requisitos para o Compartilhamento[19]

A Proposta de Resolução do BACEN que ora se examina, e que diz respeito às operações realizadas por instituições financeiras e demais instituições autorizadas a funcionar pelo BACEN[20], estabelece o consentimento expresso e prévio como uma base legal preferencial para permitir o compartilhamento de dados pessoais, além de extrapolar as hipóteses em que o consentimento é exigido na lei especial, infringindo não só a LC 105/2001, mas também a LGPD.

Um exemplo se verifica nas situações em que a proposta de Resolução do BACEN atribui ao consentimento um prazo de validade limitado a doze meses[21].

Embora essa previsão possa fazer sentido na medida em que permite ao titular dos dados uma participação mais ativa das operações realizadas com seus dados, por outro pode não ser tão salutar eis que dificulta a fluidez e continuidade das operações referentes ao *Open Banking*. O mesmo cuidado poderia ser obtido com o estabelecimento, por exemplo, de um prazo contratual a ser definido ou escolhido pelo próprio titular dos dados, não havendo necessidade de se privar de forma excessiva a livre iniciativa e a liberdade de contratar ao regulamentar o tema a essa minúcia.

---

[16] Inciso V do parágrafo 3º do art. 1º da LC 105/2001.

[17] Incisos II e VII do parágrafo 3º ao artigo 1º da LC 105/2001.

[18] Incisos III, IV, VI do parágrafo 3º ao artigo 1º 1º da LC 105/2001.

[19] Capítulos III e IV da Proposta de Resolução n. 73/2019 do BACEN.

[20] Art. 1º da Proposta de Resolução do BACEN n. 73/2019.

[21] V. Art. 10 § 1º III da Proposta de Resolução do BACEN n. 73/2019.

Com relação a outras situações relacionadas ao consentimento, o quadro comparativo abaixo demonstra alguns desencontros, a saber:

Proposta de Resolução do BACEN n. 73/2019		**Lei Complementar n. 105/2001**	
Art. 5º (c/c § 3º c/c Art. 10): exige o consentimento prévio do cliente, ou seja, antes do compartilhamento		**Art. 1º §3º**: não constitui quebra de sigilo, independente do consentimento expresso	
Inciso I: "dados sobre"	**alínea "c":** "cadastro de clientes e de seus representantes"	**Inciso 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"
Inciso I: "dados sobre"	**alínea "d":** "transações de clientes relacionadas com: (...) • item 3: "contas de pagamento pré-pagas"; • item 4: "contas de pagamento pós-pagas" • item 5: "operações de crédito"	**Inciso 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"
Inciso II: "serviços de"	**alínea "b":** "encaminhamento de proposta de operações de crédito"	**Inciso 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"

Percebe-se, assim, com mais clareza as incompatibilidades entre os diplomas confrontados acima, pelo que, para solucionar tais incongruências e evitar o risco de ilegalidades da Proposta de Resolução, o ideal seria a Proposta de Resolução fazer menção expressa à LC 105/2001, porquanto lei especial no tema à qual deve se sujeitar.

Deste modo tem-se, na presente análise, o seguinte cenário:

i. a LGPD, marco regulatório central no tema, que não estabelece hierarquia entre as bases legais que legitimam a utilização dos dados pessoais;

ii. a LC 105/2001, lei especial do Sistema Financeiro Nacional, que traz dispositivos referentes à proteção de dados pessoais ao exigir o consentimento expresso em algumas situações de compartilhamento de dados pessoais e permitir, e até exigir, o compartilhamento independentemente do consentimento[22]; e

iii. a Proposta de Resolução do BACEN que visa a regulamentar o *Open Banking,* norma infralegal especial do Sistema Financeiro Nacional, e que exige o consentimento prévio e expresso de forma incompatível com a LC 105/2001.

Já no tocante à análise da Proposta de Resolução frente à LGPD, a interpretação adequada seria: onde não houver previsão legal especial[23] a LGPD poderá regular, pelo que haverá possibilidade de utilização das outras bases legais previstas no art. 7º da LGPD para além do consentimento, como pode ser o caso de cumprimento de obrigação legal, proteção ao crédito, preliminar de contrato e execução contratual etc. Esse raciocínio, inclusive, vai ao encontro dos objetivos previstos na Proposta de Resolução, quais sejam, incentivar a inovação, promover a concorrência, aumentar a eficiência do Sistema Financeiro Nacional e promover a inclusão financeira[24].

Nessa linha de ideias, a LGPD até mesmo estabelece como uma das atribuições da Autoridade Nacional de Proteção de Dados[25]a tarefa de articular-se com entidades públicas que regulam temas setoriais de atividades econômicas e governamentais para assegurar o cumprimento das normas atinentes ao tema e promover o adequado funcionamento dos setores regulados[26]. Ou seja, a ANPD deve atuar conjuntamente com outras autoridades públicas na proteção dos dados pessoais de forma consistente e complementar, levando-se em conta que a LGPD é lei geral no tema e a ANPD é o órgão central de interpretação na matéria.

Portanto, para não se criar um precedente de enfraquecimento da LGPD e se conferir coesão e coerência ao sistema de proteção de dados pessoais sugere-se que a Proposta

---

[22] V. art. 1º §3º da LC n. 105/2001.

[23] LC 105/2001.

[24] Art. 3º da Proposta de Resolução do BACEN n. 73/2019.

[25] Órgão público cuja função precípua é zelar pela proteção dos dados pessoais, conforme prevê o artigo 55-J inciso I da LGPD.

[26] V. Art. 55-J inciso XXIII c/c seu § 3º c/c Art. 55-K c/c seu parágrafo único, todos da LGPD, a saber:

"Art. 55 -J Compete à ANPD (...) XIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; (...) § 3º 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; (...) Parágrafo único do Art. 55-K. A ANPD articulará sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação."

de Resolução faça menção expressa à LC 105/2001 e a ela se adeque, limitando a exigência do consentimento expresso para o compartilhamento de dados pessoais na forma do delineado pela LC 105/2001. Ademais, o ideal também seria a menção, igualmente expressa, à observância da LGPD naquilo que não contrariar as disposições especiais previstas nas leis que regulam o Sistema Financeiro Nacional.

4. Contratação de terceiros

A proposta ora submetida a consulta pública prevê a possibilidade de contratação de terceiros para disponibilizar aos clientes das instituições partícipes os serviços de compartilhamento dos dados e serviços de iniciação de transação de pagamento, bem como de compartilhamento de outros dados e serviços que venham a ser incluídos no escopo do sistema.

Para tal fim, não há especificidades na regulamentação proposta quanto aos tipos de produtos e serviços que podem ser prestados por terceiros às instituições contratantes, o que possibilitaria a oferta de uma ampla variedade do que pode ser objeto do contrato entre as partes. As vedações listadas limitam-se aos seguintes aspectos:

- O contratado não pode ser uma instituição regulada pelo Banco Central
- O contratado não pode atuar em nome da instituição contratante para fins de compartilhamento (ex.: a empresa contratada não pode ser a responsável direta pela disponibilização e abertura de informações e dados de clientes), e
- O contratado não pode incluir, no objeto do contrato de prestação de serviços, atividades de atendimento a clientes em nome da instituição contratante, prevista na regulamentação própria que dispõe sobre correspondentes[27]

Desta forma, entende-se que, por se tratar de um sistema de serviços de compartilhamento de dados e serviços, e de serviços de iniciação de transação de pagamento, a normativa contemplaria a contratação de **serviços relevantes de processamento e armazenamento de dados e de computação em nuvem**, uma vez que esses seriam essenciais à operacionalização da proposta tecnológica de *Open Banking* do ponto de vista técnico.

A despeito da pertinência de haver uma seção específica para tratar da contratação de terceiros no âmbito da proposta regulatória do Sistema Financeiro Aberto, foi editada, em 26 de abril de 2018, a **Resolução 4.658/2018**, que "dispõe sobre a política se segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil".

Essa Resolução prevê destacadamente a terceirização de serviços de processamento e armazenamento de dados e de computação em nuvem, no país e no exterior, por parte de instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. Especificamente, a normativa identifica o que compreendem os

[27] Banco Central do Brasil. Resolução 3.954 de 24 de fevereiro de 2011. In: https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/49450/Res_3954_v9_L.pdf

"serviços de computação em nuvem", conforme o disposto em seu art.13 e respectivos incisos, transcritos abaixo:

> *"Art. 13. Para os fins do disposto nesta Resolução, os serviços de computação em nuvem abrangem a disponibilidade à instituição contratante, sob demanda e de maneira virtual, de ao menos um dos seguintes serviços:*
> *I - processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam à instituição contratante implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela instituição ou por ela adquiridos;*
> *II - implantação ou execução de aplicativos desenvolvidos pela instituição contratante, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços; ou*
> *III - execução, por meio da internet, dos aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços."*

Essas definições apresentadas, de caráter amplo, permitem inferir que a disponibilização dos serviços de compartilhamento e de iniciação de pagamento[28], referidos na proposta de *Open Banking*, poderia ser enquadrada no escopo de contratação de terceiros da Resolução 4658, uma vez que tal disponibilização depende fundamentalmente de um aparato tecnológico (aplicativos, infraestrutura de rede, softwares) para ser, de fato, implementada.

Ademais, de acordo com o Edital 73/2019, o compartilhamento de dados e serviços, obrigatoriamente, deverá ocorrer através de interfaces dedicadas a serem disponibilizadas pelas instituições participantes, não havendo vedação quanto à possibilidade de que sejam contratados terceiros para desenvolvê-las. Os dados e serviços deverão ser "representados em meio digital e processáveis por máquina, em formato livre de restrição quanto à sua utilização"[29].

Diante do exposto, é razoável afirmar que, se aprovada nos termos atualmente propostos, a resolução que dispõe sobre o sistema de *Open Banking* Brasileiro tratará de tema já regulamentado por outra normativa já editada e em vigor, qual seja, a Resolução 4.658/2018.

Ainda assim, a Resolução 4.658/2018, por ser anterior e por trazer um rol de serviços de computação em nuvem abrangente, pode ser entendida como uma norma geral pelo Princípio da Especialidade do Direito. Para tanto, nos "casos de conflito aparente de normas, [...] a norma especial deve prevalecer sobre a norma geral"[30]. Nesse contexto, a normativa de *Open Banking* corresponderia à norma específica.

---

[28] "Serviço que inicia a instrução de transação de pagamento, a pedido do cliente, relativamente a uma conta de depósitos ou de pagamento".

[29] Edital de Consulta Pública 73/2019. Art. 23, parágrafo único.

[30] Supremo Tribunal Federal. Vocabulário Jurídico. Princípio da Especialidade. In: http://www.stf.jus.br/portal/jurisprudencia/listarTesauro.asp?txtPesquisaLivre=PRINC%C3%8DPIO%20DA%20ESPECIALIDADE

No entanto, com o propósito de garantir a segurança jurídica, bem como a manutenção de práticas harmônicas para contratação de terceiros por parte das instituições autorizadas a funcionar pelo BACEN, sugere-se a inclusão de novo artigo na Seção IV da proposta do Edital de Consulta Pública 73/2019, com a seguinte disposição:

"Aplicam-se subsidiariamente aos contratos firmados para a prestação do serviço de compartilhamento de que trata o art. 35, no que couber, as disposições da Resolução nº 4.658, de 26 de abril de 2018."

Por fim, a Brasscom gostaria de reforçar seu posicionamento já apresentado à Consulta Pública da Resolução 4.658/2018, mencionada acima. Nos preocupa essa abordagem recorrente do BACEN de acesso a contratos desta natureza e, em especial, aos códigos de acesso as informações armazenadas. No caso da Resolução sob consulta, no Artigo 37, inciso VII, dispõe-se que todos os contratos celebrados para a prestação do serviço de compartilhamento devem prever "permissão de acesso do Banco Central do Brasil aos contratos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados e aos dados ou informações sobre serviços compartilhados, bem como aos códigos de acesso a tais informações".

A Brasscom acredita que para a prestação de serviços de nuvem, assim como, para garantir a segurança, resiliência e integridade dos dados, não é necessário ter acesso a contratos, documentação e informações sobre a prestação do serviço. O acesso aos contratos não endereçará as eventuais preocupações do Banco Central com a segurança e integridade, isso será apenas alcançado através do estabelecimento de regras concretas em matéria de segurança, auditoria e integridade entre as partes do contrato, as quais poderiam ser previstas na convenção a ser firmada entre os participantes do sistema[31], que contará com a participação do Banco Central em seu processo de elaboração[32] e será, por meio da via contratual, repassada a eventuais terceiros contratos pelas entidades participantes do sistema financeiro, essas sim sujeitas à tais regras.

Ademais, gostaríamos de esclarecer que os prestadores de serviços de nuvem não possuem as chaves criptográficas do cliente. As chaves de criptografia e o acesso aos dados do cliente são feitos exclusivamente pelos próprios clientes. Assim, o Banco Central deve solicitar o acesso de dados e informações das Instituições Financeiras diretamente a elas e não aos fornecedores da nuvem. Esta obrigação de acesso aos dados e informações das Instituições Financeiras não deve fazer parte das obrigações contratuais dos fornecedores de nuvem, uma vez que esses não têm acesso a dados e informações dos seus clientes que estão na nuvem, e as chaves de criptografia que permitem o acesso aos dados pertencem aos clientes dos provedores da nuvem que, no presente caso, são as Instituições Financeiras.

5. Do Ressarcimento

[31] "Com relação à convenção, a regulamentação proposta estabelece que as instituições participantes devem formalizar instrumento para observância uniforme das questões relativas aos padrões tecnológicos e aos procedimentos operacionais, aos canais para encaminhamento de demandas de clientes, ao tratamento e à resolução de disputas entre instituições participantes, entre outros aspectos."

[32] Edital 73/2019. Art. 45.

Entendemos que o compartilhamento de dados não deve se sujeitar a um mecanismo de ressarcimento, conforme definido no Art. 41 da Resolução, visto que isso inibiria o regime de *Open Banking* no Brasil. Acreditamos que os dados deveriam ser compartilhados gratuitamente a fim de evitarmos barreiras econômicas e protegermos o acesso não discriminatório.

6. Do processo de padronização

Um aspecto que pode se tornar uma barreira para a adoção do Open Banking está relacionado à adoção de APIs pelas partes interessadas - um processo seguro pelo qual os dados são trocados digitalmente. A adoção de APIs abertas é fundamental para garantir melhor acessibilidade e acesso seguro à infraestrutura de pagamentos disponível. A adoção de APIs abertas pode melhorar a interoperabilidade e a flexibilidade das empresas para inovar e permitir que os consumidores tomem melhores decisões sobre como pagam se tiverem acesso em tempo real às informações de suas contas.

As APIs abertas e seguras permitem que vários desenvolvedores de aplicativos e provedores de serviços interajam, se comuniquem, transmitam dados e iniciem transações, colocando os consumidores no banco do motorista de suas vidas financeiras, fornecendo dados de saúde financeira em tempo real usando interfaces simples e intuitivas, ao mesmo tempo em que aumentam inclusão financeira. O fornecimento de acesso a um histórico de pagamento de aluguel em dia pode permitir que os subscritores de empréstimos ou crédito tenham uma nova visão do indivíduo e forneçam acesso a um empréstimo hipotecário residencial ou conta de cartão de crédito. Por sua vez, os credores se beneficiam de um conjunto expandido de novos clientes em potencial para atender a esses produtos e consumidores e pequenas empresas têm melhor acesso geral ao capital.

Além disso, Governos com visão de futuro em todo o mundo estão aproveitando o poder das APIs e de outras tecnologias digitais para modernizar seus sistemas de pagamentos. A interface de pagamentos unificados da Índia, uma infraestrutura construída sobre liquidação interbancária em tempo real e APIs abertas seguras, tornou-se o padrão nessa região.

Além dos desenvolvimentos na Índia, a União Europeia está no meio da implementação de APIs abertas seguras e o Ministério das Finanças do Canadá está considerando a implementação de APIs abertas seguras. Em uma economia global, derrubar barreiras para acessar serviços financeiros por meio de APIs abertas seguras permitirá ao Brasil acompanhar o ritmo de outras economias avançadas, melhorar a interoperabilidade com a infraestrutura bancária de outros países e permitir que os cidadãos brasileiros tirem vantagem de inovações em serviços financeiros que podem melhorar materialmente seu bem-estar financeiro.

Como em outras regiões do mundo[33] que adotaram o Open Banking, padrões comuns devem ser adotados no Brasil para garantir a adoção onipresente do Open Banking e a inovação contínua.

[33] Edital de Consulta Pública do Canadá: https://www.canada.ca/en/department-finance/programs/consultations/2019/open-banking.html