Instituto
de Tecnologia
& Sociedade
do Rio

Convergindo visões:

Meios de pagamento, LGPD e Impactos regulatórios

AUTORAS

Celina Carvalho, Flávia Parro Cano,
Janaina Costa e Patricia Thomazelli

EDITORES

Celina Bottino e Christian Perrone

SUMÁRIO

RESUMO EXECUTIVO

O ecossistema de meios de pagamento se expandiu muito nos últimos anos e novos atores passaram a figurar nesse mercado. Somente no setor de *fintechs*, estudos indicam uma expansão de em média 20% e muitos dos entrantes têm modelos de negócio com características específicas que os diferenciam dos participantes tradicionais. Esse é o caso dos *marketplaces*, por exemplo, que possuem entre participantes pessoas naturais.

Nesse contexto, eleva-se a preocupação da compatibilização de normas acerca da interseção entre os ecossistemas de proteção de dados e regulação do setor financeiro, especialmente sobre as obrigações de compartilhamento de dados entre atores dos arranjos de meios de pagamento.

O presente documento trata de resultados de evento promovido pelo ITS (Instituto de Tecnologia e Sociedade do RIo de Janeiro) intitulado "Convergindo visões: meios de pagamento, LGPD e impactos regulatórios"[1] em que se buscou trazer participantes especialistas nos campos de regulação de meios de pagamento e de proteção de dados. O presente documento também se apoia em análise dos ecossistema regulatório brasileiro no que tange a meios de pagamento e à proteção de dados e em um *benchmarking* de melhores práticas internacionais.

RESUMO DOS PRINCIPAIS RESULTADOS

- Há uma interação entre as obrigações oriundas da regulamentação do Banco Central do Brasil de prevenção à lavagem de dinheiro e financiamento de terrorismo e a Lei Geral de Proteção de Dados Pessoais que merece ser melhor explorada.

- É fundamental o aprofundamento do diálogo entre agentes reguladores. Promover a cooperação institucional pode ser o caminho para regulação que concilie tanto as obrigações de prevenção à lavagem de dinheiro e financiamento de terrorismo, e observância dos princípios de proteção de dados pessoais, consagrados na LGPD.

- A experiência internacional indica a necessidade de um ***"gold standard"*** de proteção de dados pessoais no contexto do processo de *compliance* para prevenção à lavagem de dinheiro e combate ao financiamento de terrorismo.

1. INTRODUÇÃO

O ecossistema de meios de pagamento se expandiu muito nos últimos anos e novos atores passaram a figurar nesse mercado. Somente no setor de *fintechs*, estudos indicam uma expansão de em média 20%.[2] A evolução do mercado trouxe entidades subcredenciadoras que mantém relação direta com os usuários finais, mas diferente dos emissores[3] e credenciadores[4], **as subcredenciadoras não necessariamente requerem autorização para funcionar pelo Banco Central do Brasil** ("BCB").[5] A configuração de seus negócios em alguns casos revela particularidades quando comparada aos modelos já existentes. Em especial, o grupo dos subadquirentes (aqueles que realizam a intermediação entre clientes e lojistas, incluindo, por exemplo, "*marketplaces*") se destaca por possuir configuração estrutural bastante heterogênea.

Na medida que as obrigações que regulam os meios de pagamento se expandem para esses novos atores, muitas vezes elas não se coadunam perfeitamente com a configuração de seus negócios. Isso se torna premente, particularmente quanto à intersecção com as obrigações de proteção de dados. Regulações do sistema financeiro muitas vezes são pensadas no sentido de obrigar o compartilhamento de dados. No entanto, esse mesmo compartilhamento pode não estar compatível com a lógica de mercado e com a regulação imposta pelo marco de proteção de dados.

Diante deste cenário, é fundamental compreender os impactos regulatórios no ecossistema de meios de pagamento com a vigência da Lei 13.079 de 2018, a Lei Geral de Proteção de Dados ("LGPD"). A interseção entre a regulamentação do setor financeiro e de proteção de dados pessoais que, em alguns momentos, pode necessitar de sintonização fina entre ambos, particularmente no que tange às especificidades de modelos de negócios inovadores, evidencia a necessidade de se conectar os diferentes agentes regulatórios para uma agenda comum.

Nessa conjuntura, com o amparo do arcabouço regulatório do BCB, **as próprias instituições credenciadoras têm demandado que as subcredenciadoras forneçam determinados dados para fins de monitoramento das execuções de obrigações legais.** Estes dados podem ser considerados dados pessoais para fins de aplicação da LGPD. O complicador nessa equação reside no fato de que, ainda, não há uma definição do BCB a respeito de quais dados podem ou devem ser requisitados das subcredenciadoras.

O presente relatório tem como propósito trazer luz com relação às potenciais tensões entre os pedidos de compartilhamento de dados (de acordo com as obrigações advindas da regulamentação do BCB) e as obrigações advindas da LGPD. Notadamente, objetiva-se fomentar o debate sobre as regras e obrigações de compartilhamento de dados entre atores dos arranjos de meios de pagamento, particularmente as obrigações de *marketplaces* que, pela configuração de seus modelos de negócio, muitas vezes acabam abarcando dados de pessoas naturais.

Tratando-se de tema complexo e ainda pouco explorado, o ITS promoveu um evento dedicado a conectar agentes regulatórios de ambos setores para reunir diferentes perspectivas, subsidiar as considerações aqui expostas e ressaltar a convergência do ecossistema de proteção de dados e a regulação do setor financeiro. O relatório, portanto, agrega explicações mais técnicas sobre o desafio enfrentado, assim como a síntese dos resultados do evento vis-à-vis a experiência internacional.

A estrutura proposta é, em um primeiro momento, brevemente trazer ao contexto os diferentes atores do Sistema de Pagamento Brasileiro ("SPB").

Em um segundo momento, passa-se à análise do fluxo de dados pessoais entre esses atores à luz do arcabouço normativo que institui as obrigações de compartilhamento discutidas.

Finalmente, mirando ao futuro, expor-se-á a complexidade regulatória trazida pelo sistema pensado do ponto de vista do atores do SPB, mas cuja centralidade nos dados torna necessária a harmonização das competências dos órgãos de regulação do setor financeiro com as funções da Autoridade Nacional de Proteção de Dados ("ANPD") estabelecida na LGPD. Para tanto, a consolidação dos resultados do evento "**Convergindo visões: meios de pagamento, LGPD e impactos regulatórios**"[6] e *benchmarking* de melhores práticas internacionais informam as convergências entre os atores e possíveis caminhos para harmonização do sistema regulatório.

2. ATORES DO SISTEMA DE PAGAMENTO BRASILEIRO (SPB)

O Sistema de Pagamento Brasileiro ("SPB") é fundado na criação dos chamados arranjos de pagamento[7], ou seja, o conjunto de regras e de procedimentos que disciplinam uma prestação de determinado serviço de pagamento ao público. Dessa maneira, as regras de um arranjo valem para todos os que aderirem ao

arranjo em si, sendo os seus participantes centrais as instituições financeiras e as instituições de pagamento.

Quanto aos participantes dos arranjos abertos,[8] estes são: (a) os instituidores desses arranjos de pagamento ("IAP"); (b) emissores; (c) estabelecimento; (d) credenciadores; (e) subcredenciadores; e (f) portadores de cartão.[9]

A. Instituidor de Arranjos (bandeiras)

São as empresas detentoras da marca e que definem quais são as regras para fins do funcionamento do sistema. Em outras palavras, **são as bandeiras de cartões de crédito**. Exemplos: Visa, Mastercard, American Express, Elo e Hipercard.

B. Emissores (bancos):

São entidades nacionais ou estrangeiras (geralmente bancos) autorizadas pelas bandeiras a emitir ou conceder cartões de pagamento. Exemplos: Banco Itaú, Banco do Brasil, Caixa Econômica Federal.

C. Credenciadores (redes):

São responsáveis por credenciar estabelecimentos de modo a permitir que esses possam aceitar cartões como meio de pagamento. São empresas que possuem uma relação com os estabelecimentos e com os emissores de cartões de forma mais direta. Exemplos: Cielo, Rede, GetNet e Stone.

D. Subcredenciadores (*marketplaces* entre outros):[10]

São responsáveis por habilitar um usuário final recebedor para a aceitação de instrumento de pagamento emitido por instituição de pagamento ou por instituição financeira participante de um mesmo arranjo de pagamento. Porém, sem participar do processo de liquidação[11] das transações de pagamento como credor perante o emissor[12]. A participação dos subcredenciadores nos arranjos abertos depende de uma escolha dos estabelecimentos envolvidos. Eles atuam como intermediários nas relações transacionais entre credenciadores e estabelecimentos. Ainda que tenham surgido, inicialmente, no ambiente virtual, os subcredenciadores têm atuado de forma cada vez mais forte no Sistema de Pagamentos Brasileiro, conquistando inclusive o espaço *offline* e constituindo um importante ator para o seu funcionamento. Exemplos: PagSeguro e Mercado Pago.

E. Estabelecimentos (prestadores de serviços e vendedores):

É provedor do bem ou serviço que firma um contrato junto a uma credenciadora ou subcredenciadora para oferecer um pagamento pelo cartão aos portadores. Exemplo: Podem ser desde pequenas empresas, como uma padaria até grandes companhias que vendam ou prestem serviço para os portadores.

F. Portadores do cartão (consumidores):

A pessoa natural ou jurídica que firma um contrato com instituições emissoras para utilizar essa modalidade de pagamento.

2.1 Os *marketplaces* dentro do Sistema de Pagamento Brasileiro

São empresas que atuam no "*e-commerce*" aproximando seus usuários compradores dos vendedores em uma plataforma colaborativa. Existem *marketplaces* que oferecem mais serviços para além da plataforma de compra e venda[13], assim como podem atuar diretamente na venda de produtos ou serviços, a depender do modelo de negócio escolhido por elas. Então, não há um modelo específico de marketplace, pode-se conjugar diversos elementos para o seu funcionamento, a conectar dois lados de uma cadeia ('*two-sided markets*"). Ou seja, permitem e apoiam transações entre fornecedores e consumidores, a oferta e a demanda[14].

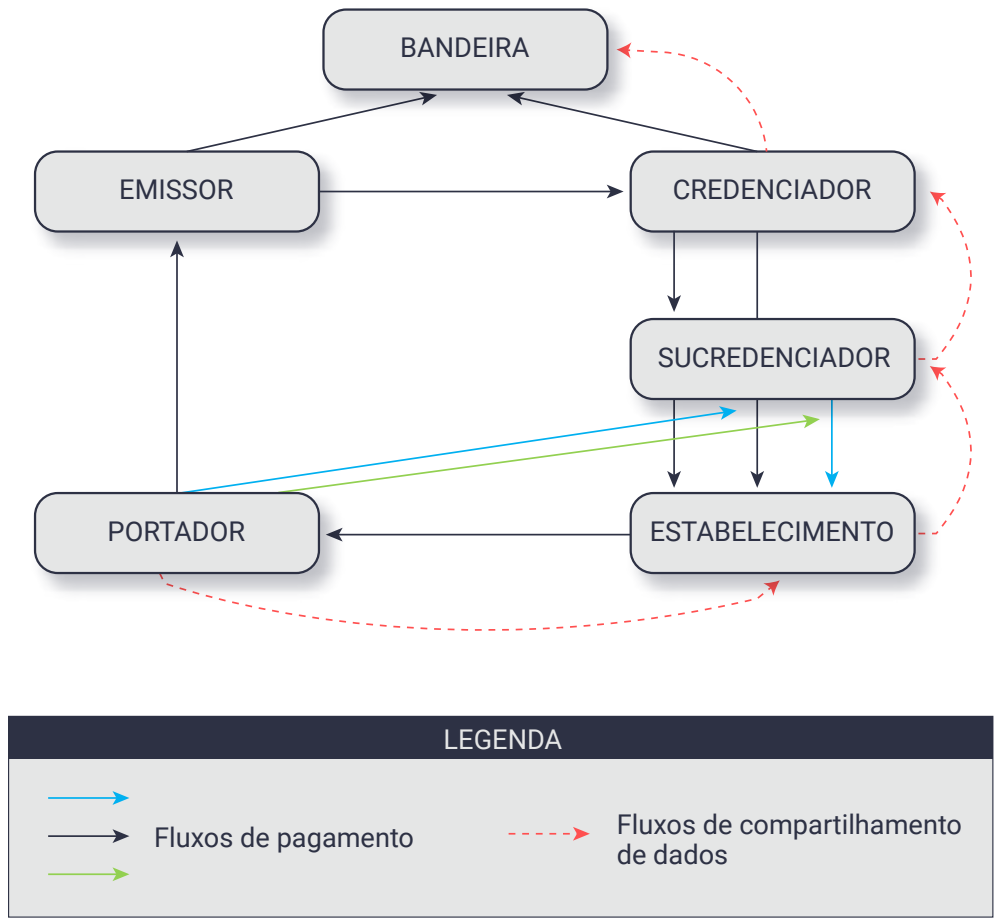
Os *marketplaces* podem atuar como subcredenciadores. No SPB, frequentemente, os *marketplaces* podem vir a atuar como subcredenciadores no recebimento e no repasse de pagamentos a vendedores após extraírem, desses mesmos fluxos, a sua própria remuneração (ex: Amazon, Mercado Livre, Uber ou iFood). Quando isso ocorre, adquirem suas responsabilidades perante o SPB, o que inclui a obrigação sobre participarem na liquidação centralizada na Câmara Interbancária de Pagamento ("CIP") em alguns casos[15].

2.2 Fluxo de Dados

Em termos de fluxos de dados, muitos dos estabelecimentos que atuam nos *marketplaces* são pessoas naturais. Estas são pessoas vendendo seus produtos ou serviços: no caso de *marketplaces* de transporte, por exemplo, são motoristas; nos de vendas, podem ser vendedores individuais; nos de serviços, podem ser *freelancers*; etc. Nesse sentido, as cadeias de compartilhamento de dados referem-se muitas vezes também a dados pessoais, atraindo a aplicação da Lei Geral

de Proteção de Dados (Lei nº 13.709/2018 ou "LGPD"), para além da regulação do Banco Central do Brasil, a ser detalhada a seguir.

Veja-se que nos arranjos de pagamentos, há uma série de fluxos de dados que se dão para garantir as próprias transações de pagamento, de forma a assegurar: (i) a prestação dos serviços que estão envolvidos no Sistema de Pagamentos Brasileiro ("SPB") e (ii) a prevenção à lavagem de dinheiro ("PLD") e a ilícitos cambiais, além dos dados compartilhados para combate ao financiamento do terrorismo[16]. O foco da presente análise se dá nesse segundo grupo de compartilhamento para prevenção de ilícitos, representados pelas setas vermelhas na figura abaixo. Serão analisadas particularmente as obrigações do art. 4º do Regulamento Anexo I da Resolução BCB nº 150/2021[17] e a Circular nº 3.978/2020.



3. OBRIGAÇÕES NORMATIVAS

Cumpre neste momento analisar o arcabouço normativo que gera as obrigações de compartilhamento discutidas.

Segundo o art. 4º do Regulamento Anexo I da Resolução BCB nº 150/2021, os instituidores de arranjos ficam obrigados a estabelecer procedimentos para atuação dos participantes no seu arranjo que contemplem:

Requisitos mínimos a serem atendidos pelos participantes e que possivelmente guardam informações dos usuários finais, sendo eles relacionados à prevenção dos ilícitos cambiais, à lavagem de dinheiro e ao combate ao financiamento do terrorismo; e, por fim

Acompanhamento de fraudes em cada instituição participante; dentre outros.

Com intuito de atingir esse fim, **os arranjos podem estabelecer diretamente obrigações aos credenciadores para monitorar o cumprimento dos requisitos postos acima por parte dos subcredenciadores**, especificando as informações que os subcredenciadores deverão franquear aos credenciadores. Essas informações não devem ser utilizadas para fins outros que não a responsabilidade de monitoramento atribuída aos credenciadores.

Assim, no cenário atual, há a exigência de que os dados necessários para a fiscalização devem ser repassados para os credenciadores. Nas resoluções do Banco Central do Brasil (BCB) **não há uma definição explícita sobre quais dados podem ou devem ser requeridos dos subcredenciadores, tampouco regulação específica acerca da proteção que deve ser prestada a dados pessoais** (em diferentes circunstâncias os dados de transações se referem a pessoas naturais que estão nos *marketplaces* prestando seus serviços ou vendendo produtos). Assim, existe a possibilidade de haver conflitos entre os pedidos de compartilhamento de dados - de acordo com as obrigações advindas da regulamentação do BCB - e as obrigações advindas da LGPD - supervisionadas pela ANPD.

Um segundo **elemento do desafio analisado se refere às obrigações trazidas pela** Circular nº 3.978/2020. A referida norma uniformizadora dispõe sobre a política, os procedimentos e os controles internos a serem adotados por instituições autorizadas a funcionar pelo Banco Central do Brasil visando à prevenção da utilização do sistema financeiro para a prática dos crimes de "lavagem" ou ocultação de bens, direitos e valores,[18] e de financiamento do terrorismo.[19]

Nem todas as instituições que fazem parte dos arranjos de pagamento precisam ser autorizadas a funcionar pelo Banco Central do Brasil.[20] Em geral, bancos, cooperativas e *fintechs* de crédito, sociedades financeiras, instituições de pagamento (em algumas situações) requerem autorização. Como os subcredenciadores não precisam necessariamente ter seu funcionamento autorizado pelo Banco Central do Brasil, em regra, não estariam sujeitos à Circular nº 3.978/2020.

No que tange a situação do compartilhamento de dados entre credenciadores e subcredenciadores, segundo o art. 31 da Circular nº 3.978/2020, caso as instituições autorizadas a funcionar pelo Banco Central do Brasil estabeleçam relação de negócio com terceiros não sujeitos a mesma autorização[21], como os subcredenciadores, e que participem de um arranjo de pagamento do qual a instituição autorizada também seja parte, **é necessário estabelecer em contrato o acesso da instituição à identificação dos destinatários finais dos recursos**, com o intuito de prevenir a lavagem de dinheiro e o financiamento do terrorismo.

Ocorre, no entanto, que os contratos entre credenciadores, bandeiras e subcredenciadores geralmente são de adesão, ou seja, os subcredenciadores acabam se sujeitando a cláusulas pré-estabelecidas, sem grandes possibilidades de alteração. Há, portanto, pouco espaço para negociação, o que afeta diretamente eventual inclusão de dispositivos específicos relacionados à proteção de dados e a LGPD pelos subcredenciadores. Assim, os subcredenciadores detém pouco espaço ou poder de barganha para incluir cláusulas que contemplem os princípios da LGPD nesses contratos.

Diante do cenário descrito, parecem haver questões de proteção de dados a serem discutidas. Há uma interação entre as obrigações que advém da regulamentação do BCB sobre combate a lavagem de dinheiro e financiamento de terrorismo e a LGPD que merece ser melhor explorada.

4. PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS A SEREM OBSERVADOS

No intuito de esclarecer como os princípios da LGPD estão relacionados com as discussões travadas, cabe explorar, de forma não exaustiva, a aplicação ao menos dos seguintes princípios: necessidade, segurança e prevenção, finalidade e adequação.

De um ponto de vista da necessidade, há que se entender como delimitar as obrigações de compartilhamento no que tange às categorias de dados que são

requeridos a guisa de satisfazer as obrigações de prevenir a lavagem de dinheiro e o financiamento de terrorismo. Sendo os *marketplaces* subcredenciadores que lidam não somente com *estabelecimentos* pessoas jurídicas, mas sim em muitos casos também pessoas naturais, há que se verificar o contexto de minimização de dados. Ainda que diversos dados possam auxiliar no processo de satisfazer o objetivo presente na regulamentação do BCB, há um possível questionamento de parte dos *marketplaces* sobre as suas obrigações de minimização relacionadas à efetiva necessidade de todas as categorias de dados informados.

Da segurança e prevenção. Sob a ótica dos princípios da segurança e prevenção, há necessidade não só de adotar medidas técnicas e administrativas aptas a protegerem os dados pessoais de acessos não autorizados, como também prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. Nesse sentido, há uma obrigação de cuidado com o fluxo de dados pessoais mesmo no caso de compartilhamento. Há que se pensar no fluxo dos dados que passam da subcredenciadora até a instituidora do arranjo de pagamento. Resta a questão se dinâmica atual, por envolver diversos agentes, sustenta-se tendo em vista os riscos para os dados pessoais que fluem na cadeia.

Com relação **aos princípios da finalidade e da adequação**, no presente contexto há uma obrigação de delimitação de uma finalidade específica, qual seja a de tratamento dos dados compartilhados, quando pessoais, de prevenção de lavagem de dinheiro e prevenção ao terrorismo (ou outros fins previamente estabelecidos na regulação que obriga o compartilhamento). Assim, os contornos do compartilhamento entre credenciadores e subcredenciadores (e os demais atores do arranjo) devem estar claros, pois de outra forma pode levar a um risco de usos outros inclusive em detrimento dos direitos dos titulares dos dados.

Sob a ótica de garantir um diálogo entre instituições e fomentar a cooperação e auxílio durante a regulação, o debate parece envolver questões sensíveis para o sistema financeiro e de prevenção à lavagem de dinheiro, assim como passa por cuidados de proteção de dados. Por isso, é essencial discutir com as autoridades competentes como identificar os caminhos convergentes que possibilitem a observância da obrigação legal em observância à proteção de dados pessoais.

Nesse diapasão, buscou-se contribuir para o fomento deste debate através do evento “Convergindo visões: meios de pagamento, LGPD e impactos regulatórios”, com a participação de especialistas dos sistemas financeiro e de pagamentos, representantes da Autoridade Nacional de Proteção de Dados (“ANPD”) e do Banco Central do Brasil (“BCB”), em que foram analisadas as regras e obrigações

de compartilhamento de dados pessoais entre atores do mercado financeiro, de pagamentos e *marketplaces* à luz da regulações pertinentes.

A seguir são apresentadas a consolidação das convergências percebidas no evento organizado pelo ITS e possíveis caminhos para harmonização e inteligibilidade da confluência de regulações sobre os diferentes atores, especialmente "*marketplaces*", tendo como cerne as obrigações de compartilhamento de dados pessoais.

5. *CONVERGINDO VISÕES:* MEIOS DE PAGAMENTO, LGPD E IMPACTOS REGULATÓRIOS

A partir da descrição sumária do cenário de atores do SBP e de regulações do setor financeiro (meios de pagamento) e de proteção de dados, nota-se que a regulação dos arranjos de pagamento, por não trazer definições específicas acerca da proteção de dados pessoais, particularmente sobre o que pode ou não ser requerido dos subcredenciadores, acaba por gerar uma potencial tensão entre sistemas de regulação dos arranjos de pagamento no que tange à proteção contra lavagem de dinheiro e financiamento do terrorismo e os mecanismos de proteção de dados.

É em relação a esse desafio que se evidencia a necessidade de diálogo entre instituições. É fundamental promover o debate informado em torno da interface entre regulação dos meios de pagamento e proteção de dados, particularmente no que tange a atores como "*marketplaces*". O desafio que se destaca é como garantir que se tenha, por um lado, o correto monitoramento do cumprimento das regras dos arranjos de pagamento com relação à observância de obrigações de prevenção à lavagem de dinheiro e financiamento de terrorismo, e, por outro, os princípios da LGPD, em especial: necessidade, segurança e prevenção, finalidade e adequação.

Diante deste cenário, o evento aberto contou com os seguintes especialistas convidados: Miriam Wimmer, Diretora do Conselho Executivo da ANPD, Isabela Maiolino, Coordenadora-Geral de Normatização da ANPD, Danilo Takasaki Carvalho, Procurador do Banco Central do Brasil, e Celina Bottino, Diretora de Projetos do ITS; e a moderação de Patricia Thomazelli, Advogada e Sócia no Rennó Penteado Sampaio Advogado.[22] Ao conectar estes *experts*, buscou-se reunir perspectivas e fomentar um debate informado, buscando ressaltar a convergência do ecossistema de proteção de dados e a regulação do setor financeiro. Focou-se nas regras

e obrigações de compartilhamento de dados pessoais entre atores dos arranjos de meios de pagamento, particularmente nas obrigações exploradas anteriormente.

5.1 Síntese do debate

Como síntese do debate travado, destaca-se posicionamentos específicos relacionados ao desafio regulatório explorado, especialmente no âmbito das informações que devem ser repassadas pelos subcredenciadores, conforme consta a Circular nº 3.978/2020. Além disso, aborda-se também os pontos de convergência mais marcantes dentre os explorados pelos participantes.

Tem-se aqui a breves apontamentos tecidos durante o evento:

A. O desafio de regulação de subcredenciadores

Os subcredenciadores nem sempre são autorizados a funcionar pelo Banco Central do Brasil, e não estão sujeitos aos diversos atos normativos que regulam o setor, o que torna a matéria complexa. O desafio, então, é alcançar os entes da cadeia que não estão obrigados a observar algumas das normas específicas. Desde do ano de 2013, a estratégia concebida pelo BCB foi construir uma estrutura pirâmide (*top-down structure*), onde o distribuidor do arranjo pode inserir regras que tratem de prevenção e lavagem de dinheiro, assim como de outras normativas de *compliance*. Dessa forma, os credenciadores permitem, através de seus contratos de adesão, a inclusão de políticas específicas.

A Circular nº 3.978/2020 traz algumas obrigações mais específicas, no entanto, concede certo um grau de autonomia para a instituição responsável pelos procedimentos de identificação de operações suspeitas do ponto de vista da lavagem de dinheiro. O objetivo é que a instituição reúna as informações para verificar operações suspeitas e, consequentemente, dar a cabo a finalidade da norma. De forma complementar, a normativa contém definições de padrões mínimos para os agentes, considerando o padrão base que o BCB espera dos agentes que supervisiona. Considerando os princípios da LGPD nesse contexto, cabe às instituições se pautarem no mínimo definido pela Circular e nos requisitos de finalidade presentes na LGPD.

Ainda em aberto está a necessidade de atualizar a Circular, quando analisada em diálogo com a LGPD. Por ora, contudo, a interpretação é de que os contratos devem seguir conforme as estipulações da lei. Isto é, os credenciadores devem

classificar e qualificar o cliente, na sequência, informar se a transação é compatível com o cliente, eventualmente assim se possa justificar uma coleta de dados mais extensiva.

No intuito de dar conforto de que haverá respeito às suas obrigações frente ao compartilhamento de dados pessoais e a LGPD, pode-se inserir os princípios da LGPD dentro das regras que disciplinam a relação com o terceiro, através do instrumento contratual.

É importante analisar o impacto da proteção de dados nessas questões caso-a-caso. Há legislações que podem parecer, prima facie, discrepantes. No entanto, não se pode esquecer que o ordenamento jurídico brasileiro funciona como um sistema. Nesse sentido, as normas de prevenção à lavagem de dinheiro do Banco Central do Brasil devem ser seguidas, assim como as da LGPD.

B. A importância do diálogo e iniciativas conjuntas entre ANDP e Banco Central

Dentre os diferentes tópicos tratados, destaca-se os apontamentos que se voltaram a afirmar a importância principalmente de um diálogo entre as autoridades regulatórias para endereçar da melhor forma a interseção da regulação do setor financeiro com a proteção de dados.

O sistema financeiro é altamente marcado pelo uso da tecnologia, e fomento de uma maior interoperabilidade com vistas a estimular a competitividade e inclusão, e que tangenciam ou mesmo tem como eixo central o uso de dados pessoais. Durante o evento, destacou-se como a regulamentação do sistema financeiro pelo BCB guarda evidente consonância com os princípios regentes da proteção de dados pessoais. Hoje, as normas mais recentes do BCB incorporam os novos conceitos que a LGPD trouxe, com destaque para o *open banking*. Temas como transparência, segurança, privacidade e não discriminação estão representados nas recentes normativas do BCB. A título exemplificativo, o princípio autodeterminação informativa é a base de criação do sistema financeiro aberto (*open banking*) e o consentimento do consumidor (titular de dados) a base legal autorizativa por excelência que possibilita a transmissão de dados que caracteriza esse sistema. Resta evidente a existência de uma perspectiva fundamental coerente com o sistema protetivo de dados pessoais e princípios corolários da LGPD.

Nesse sentido, o caminho para a promoção da cooperação institucional entre ambas instituições mostra-se aberto, especialmente para a regulação e supervisão de setores que são específicos, como é o caso do Mercado de Paga-

mentos. Somado a isso, é importante que se estabeleça iniciativas conjuntas para o aprofundamento das ações entre ANPD e o BCB.

Por um lado, neste momento em que o BCB propõem-se a buscar ativamente uma política de maior compartilhamento e interoperabilidade, pautado nas devidas proteções de dados, é possível de fato verificar o papel que a LGPD tem de promover um diferencial competitivo para as organizações que se conformarem a ela. A adequação com a LGPD aumenta a confiança ao titular de dados e pode inclusive o predispor a compartilhar seus dados com outros atores do sistema financeiro nacional.

Por outro lado, em consonância com suas atribuições elencadas na LGPD (art. 55-Jº, § 4º), a ANPD tem firmado acordos de cooperação técnica com órgãos e entidades da administração pública responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar suas competências regulatórias. A título de exemplo, a ANPD e o Conselho Administrativo de Defesa Econômica ("CADE") firmaram acordo destinado ao combate às atividades lesivas à ordem econômica e ao fomento e à disseminação da cultura da livre concorrência nos serviços que vindicarem a proteção de dados pessoais.[23] Outro exemplo que merece destaque é o acordo de cooperação técnica celebrado entre a Autoridade e a Secretaria Nacional do Consumidor ("SENACON").[24] O referido acordo tem como objetivo precípuo a promoção de ações conjuntas sobre assuntos que interessem ambos os órgãos, bem como a uniformização de entendimentos e coordenação de ações inclusive, dentre outros. Fruto desta parceria é a publicação do guia 'Como proteger seus dados pessoais', que tem como foco a conscientização do consumidor sobre a importância dos dados pessoais, além de conter orientações sobre o que deve ser feito em caso de violação que envolva o compartilhamento indevido de dados.

Considerando este ambiente, uma colaboração semelhante para harmonizar e esclarecer as regras e obrigações de compartilhamento de dados aqui discutidas, tal como **a edição de um Guia voltado principalmente para as empresas que buscam se adequar à LGPD,** poderia ser bem-vinda.

6. CAMINHOS PARA O FUTURO

Diante do exposto, nota-se que muitas das tensões mencionadas anteriormente poderiam ser minimizadas através de uma cooperação mais estreita entre a Autoridade Nacional de Proteção de Dados e o Banco Central do Brasil. Tendo-se

em vista o volume e a sensibilidade dos dados pessoais tratados no âmbito do ecossistema de meios de pagamento, a aproximação entre as instituições parece ser um caminho não só possível como provável.

O que deve se salientar é que, considerando a complexidade da discussão, inclusive a ideia de interpretação sistemática do ordenamento jurídico, a solução que a LGPD traz para esse emaranhado de normas é uma que aponta para cooperação institucional, para mecanismos permanentes de diálogo, e consultas prévias à aplicação de sanções.

Garantir um diálogo entre instituições e fomentar a cooperação e auxílio durante a regulação como elemento fundamental é uma premissa que encontra amparo também sob a perspectiva de boas práticas observadas em âmbito internacional. Ao se analisar experiência europeia, por exemplo, nota-se o posicionamento do European Data Protection Supervisor (EDPS) que defende **a necessidade de um "*gold standard*" de proteção de dados no contexto do processo de *compliance* a prevenção à lavagem de dinheiro (PLD) e combate ao financiamento de terrorismo**[25].

Mais recentemente, o EDPS publicou opinião específica[26] sobre o pacote legislativo de prevenção à lavagem de dinheiro publicado pela Comissão Europeia. De forma geral, suscitou-se definições claras, sob a perspectiva de proteção de dados, das funções de todas as partes interessadas e envolvidas no modelo de supervisão de prevenção à lavagem de dinheiro. Sobressaiu também a importância de observar os princípios da necessidade e proporcionalidade e fortalecer a segurança jurídica para entidades dos arranjos sobre seus deveres.

Nesse sentido, o EDPS trouxe recomendações específicas para o pacote legislativo analisado, dentre as quais destacamos: **(i) identificar as categorias de dados pessoais** que serão tratados por entidades para garantir a *compliance* com obrigações de PLD e combate ao financiamento de terrorismo, ao invés de deixar seja estabelecido por padrões técnicos; e **(ii) especificar quais tipos de categorias específicas de dados pessoais podem ser processadas pelas entidades envolvidas**, considerando os princípios da necessidade e proporcionalidade no decorrer das atividades e a finalidade específica.

Devido às proximidades entre os sistemas de proteção de dados brasileiro e europeu, as considerações aduzidas podem ser relevantes ao cenário aqui posto. O debate envolve questões sensíveis para o sistema financeiro e de prevenção à

lavagem de dinheiro, assim como passa por cuidados de proteção de dados, que podem ser endereçados por um diálogo institucional e iniciativas conjuntas entre autoridades competentes.

Desafios semelhantes existem na EU e no Brasil em questões relacionadas à interação entre as obrigações oriundas da regulamentação de prevenção à lavagem de dinheiro e financiamento de terrorismo e à proteção de dados pessoais. O país pode, pois, buscar inspiração em algumas das práticas adotas no contexto europeu.

Como retratado no evento, existe espaço para harmonização de regras e práticas que porventura possam justificar uma coleta de dados mais extensiva, notadamente com relação a classificação e qualificação de clientes pelos credenciadores. Nota-se que em diferentes circunstâncias os dados de transações se referem a pessoas naturais que estão nos *marketplaces* prestando seus serviços ou vendendo produtos, mas no cenário atual não há uma definição explícita sobre quais dados podem ou devem ser requeridos dos subcredenciadores pelos credenciadores, tampouco regulação específica acerca da proteção que deve ser prestada a dados pessoais.

Igualmente, maior clareza a respeito das categorias de dados pessoais tratados entre os diversos atores envolvidos nos arranjos de meios de pagamento - tal qual como preconizado pelo EDPS - parece ser chave para a compreensão das particularidades envolvidas nas referidas transações envolvendo os atores nos *marketplaces* e a harmonização desse processo de *compliance* com as obrigações de PLD e proteção de dados pessoais no contexto brasileiro.

Um dos pontos fundamentais destacado pelos *experts* convidados no evento e também respaldado pela experiência internacional resta no diálogo entre agentes reguladores. Promover a cooperação institucional pode ser o caminho para regulação que concilie tanto as obrigações de prevenção à lavagem de dinheiro e financiamento de terrorismo, e observância dos princípios de proteção de dados pessoais, consagrados na LGPD.

NOTAS

1. O evento teve como especialistas convidados Miriam Wimmer, Diretora do Conselho Executivo da ANPD, Isabela Maiolino, Coordenadora-Geral de Normatização da ANPD, Danilo Takasaki Carvalho, Procurador do Banco Central do Brasil, e Celina Bottino, Diretora de Projetos do ITS; com a moderação de Patricia Thomazelli, Advogada e Sócia no Rennó Penteado Sampaio Advogados, especialista no setor financeiro. A descrição e vídeo da gravação evento pode ser acessado através da página do ITS: https://itsrio.org/pt/varandas/convergindo-visoes-meios-de-pagamento-lgpd-e-impactos-regulatorios/.

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

3. São entidades nacionais ou estrangeiras (geralmente bancos) autorizadas pelas bandeiras a emitir ou conceder cartões de pagamento. Exemplos: Banco Itaú, Banco do Brasil, Caixa Econômica Federal.

4. São responsáveis por credenciar estabelecimentos de modo a permitir que esses possam aceitar cartões como meio de pagamento. São empresas que possuem uma relação com os estabelecimentos e com os emissores de cartões de forma mais direta. Exemplos: Cielo, Rede, GetNet e Stone.

5. É parte da missão do Banco Central do Brasil buscar assegurar a solidez do Sistema Financeiro Nacional e regular o funcionamento das entidades bancárias e não bancárias atuantes no Brasil. As Instituições de Pagamento não compõem o SFN, mas são reguladas e fiscalizadas pelo BCB, conforme diretrizes estabelecidas pelo Conselho Monetário Nacional. Vide. arts 6º, 9º e 15º da Lei nº 12.865/2013.

6. O evento teve como especialistas convidados Miriam Wimmer, Diretora do Conselho Executivo da ANPD, Isabela Maiolino, Coordenadora-Geral de Normatização da ANPD, Danilo Takasaki Carvalho, Procurador do Banco Central do Brasil, e Celina Bottino, Diretora de Projetos do ITS; com a moderação de Patricia Thomazelli, Advogada e Sócia no Rennó Penteado Sampaio Advogados, especialista no setor financeiro. A descrição e vídeo da gravação evento pode ser acessado através da página do ITS: https://itsrio.org/pt/varandas/convergindo-visoes-meios-de-pagamento-lgpd-e-impactos-regulatorios/

7. De acordo com a Lei 12.865 de 9 de outubro de 2013, que dispõe sobre os arranjos de pagamento e as instituições de pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB).

8. Os arranjos de pagamento podem ser abertos ou fechados. Num arranjo de pagamento aberto, o cartão de crédito é emitido por uma instituição de pagamento, e ele pode ser utilizado em qualquer estabelecimento, desde que a bandeira não imponha restrições. Já num arranjo de pagamento fechado, o cartão é emitido por um determinado estabelecimento (empresa de varejo, por exemplo) e somente pode ser utilizado dentro desse estabelecimento ou em parceiros do mesmo.Vide art. 2º, incisos I e II, da Resolução BCB nº 150 de 06 de outubro de 2021.

9. https://www.bcb.gov.br/estabilidadefinanceira/instituicaopagamento

10. Vide Circular 3.886/18

11. O processo de liquidação, em termos muito simplificados, seria composto por procedimentos necessários para verificar a ocorrência de uma transação de pagamento a fim de liberar o montante pago pelo portador ao estabelecimento.

12. Conforme o art. 2º, IX, do Anexo I à Resolução BCB nº 150/2021.

13. O Mercado Livre conta com o Mercado Envios, uma forma de agilizar e facilitar o transporte das mercadorias comercializadas

14. Mais informações: https://hbr.org/1994/11/managing-in-the-marketspace.

15. Conforme disposto na Circular nº 3.842/2017.

16. A lavagem de dinheiro e o financiamento do terrorismo têm a capacidade de gerar efeitos

muito prejudiciais ao SPB, ao Sistema Financeiro Nacional ("SFN") e à própria economia brasileira, tais como: a má alocação de recursos por conta de distorções nos preços relativos de ativos; bolhas de preços; equívocos na condução da política econômica por erros de medição de variáveis econômicas; alterações na demanda de moeda não relacionadas às mudanças em fundamentos econômicos; desenvolvimento de estrutura instável de ativos e de passivos nas instituições financeiras, aumentando os riscos quanto às crises sistêmicas; dentre outros.

17. A Circular BCB nº 150/2021 revogou recentemente a Circular nº 3.682/2013, repetindo, no entanto quase integralmente as disposições trazidas pelo art. 4º do Regulamento Anexo à Circular nº 3.682/2013.

18. Os crimes de "lavagem" ou ocultação de bens, direitos e valores são previstos pela Lei nº 9.613 de 3 de março de 1998.

19. O crime de financiamento ao terrorismo é previsto pela Lei nº 13.260, de 16 de março de 2016.

20. https://www.bcb.gov.br/estabilidadefinanceira/licenciamento

21. Nem todas as instituições que fazem parte dos arranjos de pagamento precisam ser autorizadas a funcionar pelo Banco Central do Brasil. Em geral, bancos, cooperativas e *fintechs* de crédito, sociedades financeiras, instituições de pagamento (em algumas situações) requerem autorização. Como os subcredenciadores não precisam necessariamente ter seu funcionamento autorizado pelo Banco Central do Brasil, em regra, não estariam sujeitos à Circular nº 3.978/2020.

22. A descrição e vídeo da gravação evento pode ser acessado através da página do ITS: https://itsrio.org/pt/varandas/convergindo-visoes-meios-de-pagamento-lgpd-e-impactos-regulatorios/

23. Disponível em : https://www.gov.br/anpd/pt-br/assuntos/noticias/act-tarjado-compactado.pdf

24. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/arquivos/acordo_anpd_senacon_assinado.pdf

25. Disponível em: <https://edps.europa.eu/press-publications/press-news/press-releases/2020/data-protection-requirements-must-go-hand-hand_en>.

26. Disponível em: <https://edps.europa.eu/system/files/2021-09/21-09-22_edps-opinion-aml_en.pdf>.

SOBRE AS AUTORAS

Celina Carvalho

Advogada. Bacharel em Direito pela Universidade do Estado do Rio de Janeiro (UERJ). Pós-graduanda em Direito Digital (UERJ). Pesquisadora da área de Direito e Tecnologia no Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio).

Flávia Parro Cano

Estagiária no Rennó Penteado Sampaio, com atuação na área de tecnologia e enfoque em proteção de dados e privacidade. É graduanda em direito na Universidade de São Paulo (USP) e realiza dupla diplomação na Université Jean Moulin Lyon 3. Foi bolsista no PET (Programa de Educação Tutorial), junto à USP, e fez intercâmbio na Universiteit Leiden na Holanda.

Janaina Costa

Advogada. Pós-graduanda em Direito Digital (UERJ); Mestre em Desenvolvimento Econômico e Social pelo IEDES - Paris 1 Panthéon-Sorbonne; Bacharel em Direito (UFMG). Ex-diretora da Diretoria de Convênios e Prestação de Contas da SEC de Minas Gerais. Pesquisadora sênior da área de Direito e Tecnologia no Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio).

Patricia Thomazelli

Graduada em Direito pela Pontifícia Universidade Católica de São Paulo (PUC-SP), Pós-graduação em Administração de Empresas pela Fundação Getúlio Vargas de São Paulo e em Direito Comercial e Arbitragem Internacional pela Queen Mary University of London. Mestrado em Creative Writing pela Kingston University, Reino Unido. Com mais de 20 anos de experiência em direito empresarial em grandes escritórios full services e em instituições financeira e de pagamentos, Patricia tem amplo conhecimento no Sistema Financeiro Nacional e no Sistema Brasileiro de Pagamentos, tendo liderado importantes projetos na área bancária, inclusive com relação ao desenvolvimento do Open Banking, à análise de produtos e serviços bancários e de pagamentos, além de compliance regulatório. Liderou projetos de adaptação de empresas do setor à Lei Geral de Proteção a Dados Pessoais, bem como de desenvolvimento de novas tecnologias aplicadas ao setor.

EDITORES

Celina Bottino

Graduada em direito pela PUC-Rio, mestre em direitos humanos pela Universidade de Harvard. Especialista em direitos humanos e tecnologia. 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. Associada do Centro de Defesa dos Direitos da Criança e Adolescentes do Rio de Janeiro. Atualmente desenvolve pesquisas na área de direitos humanos e tecnologia coordenando projetos na área de liberdade de expressão e privacidade. É afiliada ao Berkman Klein Center de Harvard e diretora de projetos do ITS.

Christian Perrone

Advogado, Consultor de Políticas Públicas. 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).

Acesse nossas redes

itsrio.org