Introdução

Não é novidade que a Lei Geral de Proteção de Dados traz grandes transformações para todas as organizações brasileiras, sendo inclusive aplicada a todas, indistintamente, até mesmo as instituições financeiras, corretoras, fintechs, cooperativas de crédito, dentre outras organizações. Apesar da massiva coletânea de leis aplicadas no setor financeiro, a LGPD não traz apenas regulamentação sobre coleta e tratamento de dados, mas também traz regras quanto à relação das empresas com seus parceiros, funcionários e fornecedores.

Toda e qualquer informação que se relacione a uma pessoa identificada ou identificável é considerada um dado pessoal. Por isso, informações de perfil comportamental, econômico, social e cadastros também se enquadram neste conceito. De outro lado, temos os dados anonimizados, sendo estas informações que não permitem identificação imediata ou posterior do titular. Como exemplo, dados sobre o percentual de homens que existem em uma carteira de clientes ou média contatada de financiamentos por pessoas de certa faixa etária são dados meramente estatísticos, que após anonimizados não podem retornar ao estado anterior, portanto, não sujeitos às regras da LGPD.

A nova lei traz novos direitos aos titulares dos dados, dentre eles a portabilidade. Este direito em particular, é relevante e oportuno diante do Open Banking, que tem como escopo a portabilidade de informações entre diferentes *stakeholders* do mercado financeiro.

Além da LGPD, outra regulamentação importante e objeto deste artigo é a Lei de Sigilo Bancário (LCP 105), que estabelece várias regras pertinentes ao dever de sigilo que as organizações do âmbito financeiro devem observar em suas operações, tanto passivas como ativas. A maior parte das informações contidas nestas operações são dados pessoais, como:

- Nome
- Endereço
- CPF/MF
- Saldo em conta corrente
- Histórico de movimentação financeira
- Contratação de produtos e serviços financeiros

A violação do sigilo estabelecido pela LCP 105 é punida com reclusão de um a quatro anos e multa, sem prejuízo de punições na esfera civil e administrativa, com possibilidade de pagamento de indenização. Neste sentido, o dever de sigilo apenas poderá ser quebrado em hipóteses previstas na LCP 105, em casos de comunicação de ilícitos penais ou administrativos, terrorismo, tráfico de entorpecentes, lavagem de dinheiro, entre outros.

Contudo, como adentrar às inovações trazidas pelo Open Banking sem violar a Lei de Sigilo Bancário?

É o que veremos adiante.

Open Banking

Sabemos que o setor financeiro aqui no Brasil é muito concentrado em poucos agentes econômicos. Visto os impactos negativos que isso pode trazer para a economia, o Banco Central do Brasil ingressou na jornada de maior integração regulatória para que nosso país tenha mais *players* no mercado. Para tanto, o Banco Central estruturou um modelo jurídico de Open Banking.

Essa nova iniciativa pressupõe a abertura de dados de clientes de determinada instituição financeira ou instituição regulada pelo Banco Central, compartilhando esses dados cadastrais e dados de operações financeiras com outras organizações que participem deste sistema, por meio

de uma grande interoperabilidade de sistemas.

O comunicado nº 33.455 de 24 de abril de 2019, detalhou os requisitos mínimos para que o Open Banking seja implementado no Brasil, sendo que em 4 de Maio de 2020, o Banco Central publicou a Circular nº 4.015 e a Resolução Conjunta nº1, e listou os dados que deverão ser compartilhados pelos participantes, sendo eles:

- Cadastro de clientes, compreendendo, no mínimo, os dados de identificação do cliente exigidos pela regulamentação em vigor, qualificação pessoal do cliente e outras informações cadastrais como data de início do relacionamento com a instituição, identificação da agência e conta, tipos de produtos e serviços com contratos vigentes e poderes dos representantes, se houver;

- Dados sobre transações de clientes, compreendendo, no mínimo:

→ Em contas de pagamento à vista, poupança e pré-pagas: o tipo de conta, saldo, e transações realizadas (com identificador da transação, valor, data, pagador e recebedor), débitos e pagamentos autorizados (com valor, data e recebedor), limite de cheque especial (com valor utilizado e valor disponível);

→ Em contas de pagamento pós-pagas: tipo de conta, limite de crédito total (com valor utilizado e valor disponível), limite de crédito por modalidade de operação (com valor utilizado e valor disponível), transações de pagamento realizadas (com identificador da transação, valor, data e recebedor), informações sobre o pagamento da fatura (com data do vencimento, data do pagamento efetivo, valor total da fatura, valor de pagamento da fatura, forma de pagamento e encargos cobrados);

→ Operações de crédito: modalidades de operações de crédito, número do contrato, data da contratação, valor da operação, data de vencimento, data dos respectivos pagamentos, saldo devedor, prazo total e remanescente da operação, quantidade de prestações, valor das prestações, taxas de juros remuneratórios anula, nominal e efetiva pactuadas, Custo Efetivo Total (CET), sistema de pagamento, tarifas e encargos.

Grande parte dos dados supracitados são protegidos pela Lei do Sigilo Bancário. No entanto, a própria lei traz em seu artigo 1º, §3º, que as informações financeiras podem ser compartilhadas com terceiros, desde que haja o consentimento do interessado.

Consentimento

Na mesma linha da Lei do Sigilo Bancário, a Resolução Conjunta dispõe que o compartilhamento de dados de clientes voltados para a iniciativa do Open Banking apenas poderá ocorrer caso haja o consentimento, sendo este definido pela Resolução como uma manifestação livre, informada, prévia e inequívoca de vontade, feita pelo meio eletrônico, pela qual o cliente concorda com o compartilhamento de dados ou de serviços para finalidades determinadas.

Por isso, diferentemente do que dispõe a LGPD sobre a autorização do tratamento de dados pessoais em outras bases legais além do consentimento, aqui no sistema de Open Banking, a portabilidade dos dados sempre necessitará o consentimento do titular.

Além disso, a Resolução Conjunta discorre sobre algumas características peculiares deste consentimento, devendo este ser:

- Solicitado com linguagem clara e adequada;
- Referir-se a finalidades determinadas;
- Ter prazo de validade compatível com as finalidades, limitado a doze meses;
- Discriminar a instituição transmissora de dados ou detentora da conta, conforme o caso;
- Discriminar os dados ou serviços que serão objeto de compartilhamento;
- Incluir a identificação do cliente;

- Ser obtido após a data de entrada em vigor da Resolução Conjunta e
- Tendo alterações das condições do segundo ao quinto item, novo consentimento deverá ser obtido.

Sendo vedado obter o consentimento do cliente:

- Por meio de contrato de adesão;
- Por meio de formulário com opção de aceite previamente preenchida ou
- De forma presumida, sem manifestação ativa do cliente.

Devendo a organização participante informar ao cliente, no mínimo:

- A identificação das instituições participantes;
- Dados e serviços objeto do compartilhamento;
- Período de validade do consentimento;
- Data de requisição do consentimento;
- Finalidade do consentimento, no caso em que a instituição em tela seja iniciadora de transações de pagamento ou receptora de dados.

Seguindo ainda a linha da LGPD, a resolução dispõe que o consentimento poderá ser revogado, a qualquer tempo, por meio de um processo seguro, ágil, preciso e conveniente, sendo essa revogação disponível no mesmo canal de atendimento no qual ele foi concedido, se ainda existir. O prazo de retenção do consentimento, registros de acesso e sua revogação devem ser guardados por um prazo mínimo de 5 (cinco) anos.

O compartilhamento dos dados em questão poderá ser feito entre parceiros de negócio, ainda que não regulados, desde que também haja o consentimento do cliente, com medidas organizacionais e cláusulas contratuais específicas, ditadas pela Resolução Conjunta.

Auditorias, testes, definição de processos, métricas, dentre outros, são mecanismos dispostos na Resolução para garantir a confiabilidade, disponibilidade, segurança, integridade e sigilo dos processos envolvidos no Open Banking, incluindo o consentimento, sendo sua autenticação, confirmação e revogação sujeitos a essas medidas.

Conclusão

Percebemos que a Lei Geral de Proteção de Dados, no caso do compartilhamento de dados para fins de Open Banking, caminha juntamente com a inovação, instituindo a privacidade e proteção dos dados como um padrão deste novo sistema.

As instituições financeiras que desejam ser parte desta nova iniciativa, além de estarem adequadas à lei, também deverão adequar seus processos internos e sistemas para que atendam às expectativas da lei e resoluções, sendo questão central o respeito aos novos direitos dos titulares trazidos pela LGPD.

A Lei de Sigilo Bancário também abriu espaço para uma interpretação nova, não mais correndo o risco de haver sua violação e não mais sendo um entrave para que a nova sistemática financeira funcione em nosso país, deixando cada vez mais simples e facilitado o acesso a novos produtos e serviços que as instituições têm a oferecer no mercado.

Autores: Milena Pappert, Flávia Alcassa e Hiran Cruz- Escritório Alcassa & Pappert Advogados

Referências

Temas atuais de proteção de dados [libro eletrônico]. -- 1. ed. -- São Paulo : Thomson Reuters Brasil, 2020.

BRASIL. Banco Central do Brasil. Comunicado nº 33.455, de 24 de abril de 2019. Disponível em http://www.in.gov.br/web/dou/-/comunicado-n%C2%BA-33.455-de-24-de-abril-de-2019-85378506. Acesso em 13 de janeiro de 2021.

Edital 73/2019. Disponível em https://www3.bcb.gov.br/audpub/DetalharAudienciaPage?11&pk=322. Acesso em 13 de janeiro de 2021.

Resolução Conjunta nº 1, de 4 de maio de 2020. Disponível em https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/51028/Res_Conj_0001_v1_O.pdf. Acesso em 14 de janeiro de 2021.

Lei nº 13.709 de 14 de agosto de 2018. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em 14 de janeiro de 2021.

UNIÃO EUROPEIA. Parlamento Europeu. (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679. Acesso em 15 de janeiro de 2021.