Luz e Teófilo: LGPD subiu a barra das contratações?

Todas as organizações que realizam o tratamento de dados pessoais no Brasil, de indivíduos localizados no Brasil, ou cujo tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços, devem

Proteção de Dados Pessoais (LGPD).

Para isso, a LGPD estabeleceu uma sistemática normativa própria baseada em conceitos como *dado pessoal*, *titular*, *tratamento* de dados, *agentes de tratamento* , além de determinar direitos e obrigações. Outro ponto fundamental foi a definição de autoridade pública especializada para regular e guiar o entendimento sobre o assunto no país, com a possibilidade de aplicação de sanções que incluem multas calculadas sobre o faturamento, publicização da infração e até proibição da atividade envolvida na violação.

Pode-se observar neste primeiro ano de vigência um grande divisor de águas, vez que não se contava, até então, com semelhante e tão abrangente regulação sobre o uso de dados de pessoas no Brasil, em ambiente onde havia somente disposições esparsas e setoriais [1].

Entre as consequências de infrações à LGPD, está a possibilidade de aplicação de sanções administrativas, cujas regras figuram no processo administrativo sancionador, publicadas em 29 de outubro de 2021, conforme Resolução CD/ANPD nº1.

Segundo pesquisa realizada pela Fundação Dom Cabral [2], de agosto de 2021, cerca de 40% das empresas dizem não estar preparadas para a entrada em vigor das penalidades previstas pela LGPD. A pesquisa aponta ainda que 61% dos Conselhos reconhecem que a LGPD traz valor para as empresas e não a veem como mais um obstáculo burocrático.

Na prática, uma única organização não é capaz — e nem seria interessante do ponto de vista econômico e de eficiência — de realizar todas as atividades que envolvem de alguma forma dados pessoais. Por isso, estabelece relações com outras instituições que atuam na condição de operadoras ou também de controladoras.

São empresas de marketing, fornecedores de sistemas, escritórios terceirizados e parceiros de negócios que prestam diferentes serviços, naturalmente enquadrados como *tratamento* de dados pessoais.

A contratação de parceiros de negócios é natural e necessária. Pode-se citar como exemplo a formalização de contratos já prevendo exigências sobre proteção de dados pessoais [3] desde o edital de licitação [4] pelo Poder Judiciário de Santa Catarina.

Por isso, é relevante a gestão destas relações também em termos de proteção de dados, acrescidos de outros aspectos que já são analisados e validados nas diligências pré-contratuais.

Ora, de nada adianta o investimento num programa de governança em privacidade interno caso os dados de clientes sejam compartilhados com outra organização que não possui o tema como pauta e possa expor estes titulares a riscos.

As sanções em potencial para as infrações à lei, somada ao próprio risco de impacto reputacional e de judicialização, tornam de suma importância o questionamento sobre com quem compartilhar dados pessoais e a necessidade de tal compartilhamento, para evitar envios desnecessários e, por consequência, riscos desnecessários.

Due diligence em proteção de dados

É recomendável que a contratação ou renovação de contratação com terceiros seja precedida de um processo de *due diligence* (diligência prévia), por meio do qual são coletadas informações para subsidiar a tomada de decisão quanto ao seguimento ou não em determinada negociação.

Em muitas organizações, esta prática já é recorrente e compõe a cultura organizacional, e que agora vem acrescida da abordagem de questões sobre proteção de dados pessoais e segurança.

Nesta etapa pré-contratual, busca-se entender de que forma o terceiro pode fornecer garantias adequadas aos dados pessoais que for tratar. Esta diligência pode incluir a verificação de: medidas de segurança da informação adotadas, *frameworks* aplicados, treinamento e capacitação de colaboradores, adoção de cláusula de confidencialidade, uso de serviços de outras organizações, localização do armazenamento de dados (e, particularmente relevante se houver transferência internacional de dados), apenas para citar alguns exemplos.

Tais verificações, se serão mais ou menos aprofundadas, dependerão do papel do agente de tratamento que se pretende contratar. Isto é, do que efetivamente ele estará incumbido de realizar na cadeia de tratamento de dados pessoais e qual o respectivo risco desta operação em relação aos titulares dos dados.

Agentes de tratamento e atribuição de papéis

Juntamente da diligência prévia e optando-se pelo estabelecimento da relação com o terceiro, deve estar claro com qual tipo de *agente de tratamento* se está a lidar: se *operador* ou *controlador*.

Pela definição legal, controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Segundo a ANPD [5], este papel pode decorrer de obrigações expressas em norma jurídica ou de contrato firmado entre as partes.

Já o operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, segundo as instruções fornecidas por este.

Novamente em remissão à ANPD, *"a principal diferença entre o controlador e operador, qual seja, o poder de decisão: o operador só pode agir no limite das finalidades determinadas pelo controlador"* [6].

A definição do agente de tratamento nem sempre se apresenta de forma simples, demandando análise quanto aos papéis desempenhados por cada um e, para isto, remetemos ao guia orientativo da ANPD referido acima.

Podemos vislumbrar ainda a existência das figuras de suboperadores e de controladores conjuntos. Contudo, todos estes são conceitos funcionais, de modo que são estabelecidos de acordo com a real atividade praticada por cada agente, pouco importando que o contrato disponha de forma diversa — e equivocada, diga-se.

Por exemplo, uma organização que atua definindo a finalidade do tratamento não pode denominar a si mesma em contrato como operadora, da mesma forma que alguém denominado formalmente operador não pode atuar com poder de decisão sobre a finalidade do tratamento.

O efeito prático disso é o reflexo direto no regime de responsabilidade entre as organizações, na medida em que o controlador é o principal responsável pelo tratamento, enquanto que o operador responderá na condição de controlador em caso excepcional, quando descumprir a lei ou atuar em desconformidade com as instruções lícitas do controlador.

Portanto, previamente à disponibilização do próprio acesso a dados pessoais, é importante que seja estabelecido um acordo com o terceiro, que estipulará as condições relativas ao tratamento e segurança destes dados. Este instrumento contratual, por sua vez, deve ser capaz de delimitar com precisão entre as partes o escopo do tratamento dos dados por cada agente e a responsabilidade.

Dentre os elementos que podem vir a compor este acordo de tratamento de dados pode-se mencionar:
— o objeto e a duração do tratamento;
— a finalidade do tratamento;
— o tipo de dados pessoais;
— as instruções do controlador;
— a adoção de medidas de segurança;
— cooperação com o controlador em caso de incidentes e exercício de direitos de titular;
— a possibilidade de contratar ou não um suboperador [7];
— cumprimento de políticas do contratante;
— existência de transferência internacional de dados;
— possibilidade de realização de auditoria pelo contratante;
— apagamento ou devolução dos dados pessoais.

Uma vez mais ressaltamos que a complexidade da análise e do próprio contrato dependerá da operação de tratamento de dados que efetivamente pretende-se que o parceiro de negócio realize. Quanto maior o risco da operação de tratamento a ser realizada, maior atenção à definição das especificidades no contrato.

Conclusão
Em que pese os desafios imanentes da adequação à LGPD, os mais variados segmentos econômicos já reconhecem a relevância do tema e passaram a exigir de seus parceiros comerciais semelhante comprometimento.

A proteção de dados impactou as relações comerciais de modo que organizações preocupadas com o respeito à privacidade e proteção de dados tendem a só fazer negócios com outras que também tenham o tema como pauta e estejam aptas a garantir a segurança dos dados pessoais que forem objeto de seus contratos.

A partir daí, estas relações devem ser gerenciadas, de acordo com as cláusulas estipuladas entre as partes, observando-se, ao seu encerramento, a destinação final dos dados pessoais tratados por cada agente.

Desta forma, pode-se concluir que estar em conformidade com a LGPD tornou-se também uma necessidade para se manter relevante no mercado — ou mesmo uma questão de sobrevivência. Em outras palavras, aquele que oferta seus produtos e serviços deve estar ciente que a conformidade tornou-se requisito para a concretização de negócios.

[1] Vide disposições no Código de Defesa do Consumidor, limitadas às relações de consumo, na Lei do Cadastro Positivo, na Lei de Acesso à Informação, no Código de Ética Médica e algumas regulações infralegais.

[2] FDC. Pesquisa A LGPD, o Conselho e a adequação das empresas à lei. Disponível em: https://www.fdc.org.br/Documents/LGPD_-_Relatorio_de_Pesquisa.pdf Acesso em 15 fev. 2022.

[3] https://www.tjsc.jus.br/web/imprensa/-/pjsc-formaliza-primeiros-contratos-de-acordo-com-a-lei-geral-de-protecao-de-dados. Acesso em 17 fev. 2022.

[4] http://www2.tjsc.jus.br/web/cache/sistemas/licitacao/download/ebipjmlqxw/20210001.pdf. Acesso em 17 fev. 2022.

[5] ANPD. Guia Orientativo para Definições dos Agentes de Tratamento. p. 7

[6] Idem. p. 16

[7] Esta possibilidade é vislumbrada pela ANPD: *"o suboperador é aquele contratado pelo operador para auxiliá-lo a realizar o tratamento de dados pessoais em nome do controlador"*. Idem. p. 19.

Date Created
01/04/2022