Por Marcos Bentes (*)

Agosto de 2020 chegou e com ele, a expectativa da entrada em vigor da Lei Geral de Proteção de Dados (LGPD), Lei 13.709/2018. Há certa indefinição e expectativas quanto à Lei se tornar realmente efetiva neste mês, considerando o cenário – realmente ainda existem algumas dúvidas com a Medida Provisória nº 959 de 2020 e prorrogação das sanções administrativas pela Lei nº 14.010, de 2020, o que traz incerteza ao cenário já complexo.

Entretanto, a tendência da LGPD tornar-se efetiva parece um caminho sem volta. Olhando nosso entorno, uma maior demanda por proteção de dados pessoais não se limita apenas ao Brasil. É um debate global em que o Brasil está inserido. A adoção de legislações de privacidade em outros países vem demonstrando a consolidação de uma tendência global, como por exemplo, movimentos recentes ocorridos em vizinhos, tais como no Chile e em países mais distantes como Coréia do Sul, Japão, Quênia, Índia, Indonésia, Califórnia (EUA), além da União Europeia.

Privacidade é um direito fundamental e indivíduos em todo o mundo valorizam cada vez mais a privacidade e a segurança de suas informações. Em uma economia cada vez mais baseada em dados, incluindo os pessoais, a LGPD é essencial para garantir que os indivíduos tenham melhor controle sobre suas informações e que essas sejam processadas com uma finalidade legítima, legal e justa. Por outro lado, com a LGPD, o Brasil passou a integrar a relação de países que contam com uma lei ampla e bem estruturada e protelar a efetividade da Lei além de 2021, que se aproxima de forma acelerada, pode não ser uma opção.

Nesse sentido, mesmo com uma eventual postergação da LGPD, privacidade, proteção de dados, garantia do exercício de direitos individuais dos titulares, a definição e correta divisão de responsabilidades entre controladores e operadores de dados, tratamento de dados sensíveis, bem como outros itens, são temas de negócios relevantes que já estão ou deveriam estar nas agendas das organizações. Por exemplo, há de se ressaltar que os Princípios de Privacidade Geralmente Aceitos (GAPP) foram desenvolvidos em 2009 pelas instituições AICPA (EUA) e CICA (Canadá) e foram divulgados amplamente desde então. Por outro lado, a GDPR (Lei de Proteção de Dados da União Europeia) já está efetiva desde 2018.

Mesmo com todo esse movimento global e local, que não é recente como discutimos acima, apostar em uma postergação da LGPD como razão principal para não iniciar ou mesmo adiar a continuidade dos esforços de conformidade com a Lei não seria uma decisão coerente. O compliance, com a LGPD, exige recursos tecnológicos, pessoais, financeiros e o mais importante, tempo. Nesse sentido, para auxiliar as organizações na reflexão de seu risco de atendimento de compliance com a LGPD, que já deveria ter sido atingido em agosto de 2020, elencamos 10 questões, que costumamos dizer ser um “teste de realidade”, ou seja, uma avaliação da situação/cenário atual:

1 - Foram definidas e documentadas as políticas de privacidade bem como políticas de segurança relevantes para proteção de informações pessoais?

2 - Foram definidas as responsabilidades, níveis de autoridade e a governança interna sobre privacidade, com envolvimento da alta liderança (diretoria, comitê, etc)?

3 - Foram realizados inventário, identificação e classificação da informação pessoal utilizada pela organização?

4 - Um programa de gerenciamento de incidentes de privacidade foi definido, incluindo políticas, procedimentos e responsabilidades?

5 - O uso, retenção e expurgo de informações pessoais já foram considerados?

6 - Ações e programas de treinamento e conscientização sobre privacidade foram realizados para todo o pessoal da organização?

7 - As bases legais que fundamentam a coleta dos dados foram compreendidas e planos de ação foram preparados, quando aplicável?

8 - Processos e meios de fornecer acesso dos titulares aos seus dados já foram considerados?

9 - Relacionamentos com terceiros que envolva acesso, uso e/ou divulgação de dados pessoais já foram mapeados e revisados sob a ótica de privacidade?

10 – As necessidades de melhoria da segurança do ambiente tecnológico para privacidade dos dados já foram identificadas e estão sendo tratadas?

Se você leitor respondeu “não” a alguma das perguntas do teste acima, seu programa de privacidade está em risco e o possível adiamento da LGPD deveria ser utilizado para canalizar os esforços em prol da aceleração e estruturação do programa de privacidade da sua organização.

Se respondeu “talvez”, “temos que confirmar”, ou seja, se está inseguro sob o nível de efetividade, é recomendável realizar uma análise de lacunas (gaps). Se respondeu “sim” com convicção a todas as perguntas, parabéns! Entretanto, convém utilizar o tempo ainda disponível para testar e efetuar uma última revisão da efetividade de seu programa, pois o assunto é complexo e eventuais ajustes ainda podem ser necessários.

(*) **Marcos Bentes** é sócio da área de Risk Advisory Services (RAS) da consultoria RSM Brasil (Acal).

Fonte: O Estado de S. Paulo, em 25.08.2020