Por Marília Kairuz Baracat (*)

Muito tem se falado e escrito sobre a importância de protegermos a privacidade das pessoas na era da informação. O dado, a informação, seja ela pública, privada, difundida em meio físico ou lógico, merece proteção legal. Nos casos dos dados pessoais, sejam eles sensíveis ou não, carecem de cuidados redobrados por todos aqueles que tratem os dados. Em linhas gerais, tratamento de dados engloba todas as ações que se realizam com os dados: coleta, armazenamento, mineração, descarte, dentre outras formas.

Em uma sociedade globalizada, com interações digitais crescentes, urge que se protejam os dados das pessoas para que não se incorra na exposição da privacidade e intimidade delas, ferindo seus direitos mais fundamentais.

E nesta sociedade dos dados, com tantas interações e produções de insights pelas empresas, constata-se que para estas se adequarem à LGPD– Lei Geral de Proteção de Dados, é preciso um projeto bem estruturado, requerendo profissionais especializados, treinados e com diferentes visões, já que o tema é multidisciplinar. Acredita-se que o período de vacatio legis da LGPD deva ser encarado como uma oportunidade para as empresas iniciarem suas discussões internas, aprovarem seus orçamentos para 2020, contratarem profissionais especializados e, assim, poderem em um curto espaço de tempo, produzirem seus relatórios de impactos à proteção de dados [**1**] (ou DPIA).

Uma das obrigações das empresas inseridas no bojo da LGPD é a elaboração do Relatório de Impactos à Proteção de Dados. Este documento consiste na análise dos impactos dos dados pessoais em uma organização. É por meio de uma análise de riscos dos mesmos que se inicia tal processo. Os riscos são muitos e variados: dados expostos indevidamente, vazados ou descartados incorretamente.

No entanto, diante de nossa experiência em temas transversais, aconselha-se que a análise de riscos seja feita considerando-se os processos, os fluxos dos dados pessoais na organização, por onde os dados entram, qual o caminho que percorrem e qual o destino deles, independentemente de estarem armazenados em meio físico ou digital.

Tendo uma visão de processo dos dados pessoais na empresa, poderemos partir para a análise de riscos. Quando se fala em impacto de algo ocorrer, há que se considerar a probabilidade de acontecer. Um risco pode ter impacto altíssimo e baixa probabilidade de ocorrer. Então, conclui-se que a análise de riscos é relacional. Dessa forma, enseja que análise a ser feita garanta um nível de discussão acerca do risco, com os vetores “probabilidade” e “impacto” muito bem dimensionados.

Salienta-se que para se ter sucesso na análise dos riscos, os profissionais que a realizam precisam contar com a participação dos proprietários do risco. Por exemplo, um risco de TI precisa ser discutido e analisado por profissionais de TI. Certamente, profissionais com outras expertises também são bem-vindos, como os do jurídico, compliance e privacidade.

Mas, afinal, o que é risco?

De acordo com o conceito da norma técnica ISO 31000 que regula a matéria, risco é o efeito da incerteza nos objetivos.

Depreende-se que o ideal, antes de iniciarmos o gerenciamento de riscos, é termos um planejamento estratégico da empresa atualizado, com os objetivos estratégicos alinhados à missão e visão da empresa.

Assim, um determinado risco da empresa será o efeito da incerteza para o cumprimento de um objetivo estratégico. É certo, pois, que há riscos estratégicos e operacionais. Nesse sentido,

recomenda-se que se inicie a gestão de riscos pelos estratégicos, pois são os que podem comprometer a razão de existência da empresa.

Ademais, o impacto de um risco estratégico acontecer provavelmente será mais gravoso para a empresa do que a ocorrência de um risco operacional.

É vital começarmos a organizar melhor as corporações em termos de processos e de análise de riscos. Dessa forma, conheceremos os riscos associados ao cumprimento da LGPD e poderemos nos preparar melhor para tal.

Tudo isto servirá de base para a elaboração do relatório de impactos à proteção de dados.

Em resumo, importa menos saber a data exata do início de vigência da LGPD, pois conforme demonstrado acima, já há muito a ser feito pelas organizações no sentido de preparar as empresas para os desafios colocados na LGPD.

[**1**] Art. 5º/LGPD. Para os fins desta Lei, considera-se: XVII – relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

(*) **Marília Kairuz Baracat** é head de Privacy e Compliance do escritório Di Blasi Parente & Associados.

Fonte: O Estado de S. Paulo, em 18.11.2019