Por Paulo França (*)

Sancionada em 2020, a LGPD (Lei Geral de Proteção de Dados) continua trazendo dúvidas e incertezas sobre qual a forma correta de se adequar e quais passos devem ser seguidos para minimizar a exposição de dados. Isso acontece devido ao fato de que nunca houve uma legislação que remetesse a tantas disciplinas diferentes, envolvendo não só pilares jurídicos, como também de governança, cultura, processos, controles, tecnologia e segurança da informação, além dos seus respectivos subprocessos.

O primeiro passo das empresas, que começou no segundo semestre de 2020, e continuou nos seis primeiros meses de 2021, foi o de olhar a adequação sob o aspecto jurídico, ou seja, fizeram uma avaliação e criaram um plano de adequação para minimizar riscos legais e fazer o mínimo necessário para poder ter uma resposta em eventual solicitação do órgão regulador, a ANPD (Autoridade Nacional de Proteção de Dados Pessoais). Passada essa fase, agora já acompanhamos organizações se movimentando para implantar controles, ou seja, tecnologias e ações que buscam minimizar os riscos envolvendo esta disciplina, até então não tratada.

É válido afirmar que, assim como as necessidades jurídicas não têm uma resposta padrão e dependem de uma análise de cada empresa, a tecnologia também deve servir a essas particularidades. Um trabalho coeso de adequação à LGPD envolve, entre outras atividades importantes, o foco na análise de riscos atrelados às fragilidades que a empresa naturalmente possui e que merecem uma investigação própria e minuciosa.

Sabendo quais são as suas fragilidades e quais os riscos a empresa está correndo, fica muito mais fácil e menos custoso fazer um plano de ação que vise diminuir as preocupações. A empresa pode se valer tanto de ferramentas simples que já existem no mercado ou desenhar uma solução própria

de acordo com suas necessidades. Por isso, o primeiro passo é procurar auxílio de profissionais qualificados com experiência em tecnologia e LGPD. Num segundo momento é chegada a fase de análise de cada necessidade e particularidade da empresa para, só depois, tomar a melhor decisão.

Em relação à coleta de dados, a empresa deve demonstrar visibilidade, transparência, intenções e motivações de seus processos, mas sigilo total no armazenamento e processamento. Ou seja, quando um titular disponibiliza seus dados a uma empresa, ele deve saber o que será feito com as informações e quais vantagens ele terá nessa operação, bem como se certificar de que outras pessoas envolvidas não terão acesso a esses dados. Desta forma, o dado tem seu ciclo de vida completo, no qual é coletado, utilizado e posteriormente excluído.

Hoje, toda empresa deve conhecer com exatidão o ciclo de vida dos dados pessoais e sensíveis que fazem parte da sua operação. Com esse conhecimento em mãos e entendendo o nível de exposição ao risco referente às áreas de tecnologia e segurança da informação sobre cada etapa do ciclo de vida, a organização poderá então avaliar quais as melhores tecnologias que atendem às necessidades de proteção dos dados durante este ciclo, entendendo os riscos, as arquiteturas, as integrações e as plataformas, entre outros. Vale lembrar que não existe receita de bolo ou um software específico que fará tudo isso, mas sim conceitos, tecnologias, e diversos serviços e frameworks que, isoladamente ou em conjuntos parciais, poderão atender na medida as necessidades do negócio.

Vale ressaltar que, sejam quais forem as necessidades da empresa, todo cuidado é pouco e as ações devem ser tomadas. Gigantes da tecnologia como LinkedIn e Twitter tiveram dados violados, informações sobre compradores de ingressos da Olimpíada de Tóquio foram distribuídas e milhões de dados pessoais de brasileiros vazaram e ainda não se tem certeza qual a origem desse acontecimento.

Mas, a pergunta que fica é se isso pode acontecer com sua empresa. Claro que boa parte do esforço em sequestrar dados pode estar atrelado ao dinheiro, mas em alguns ataques as motivações são diferentes. O hacker que vazou dados de 700 milhões de usuários, por exemplo, diz ter feito isso por diversão. Já a plataforma Lattes pelo CNPq (Conselho Nacional de Desenvolvimento Científico e Tecnológico) saiu do ar por uma falta de manutenção dos equipamentos, por meio de um servidor desconectado.

Como, então, saber medir o investimento suficiente que garanta segurança e não inviabilize as operações? Conduzindo um processo de adequação e manutenção da LGPD de maneira responsável e com profissionais qualificados para que as tecnologias aplicadas sejam as mais eficientes e menos custosas e possam garantir a proteção de clientes, funcionários e stakeholders.

(*) **Paulo França** é gerente de Digital Consulting and Innovation da Engineering, companhia e consultoria global de Tecnologia da Informação especializada em Transformação Digital.

Fonte: IMAGE, em 12.08.2021