

Por Ana Albuquerque (*)



Com a vigência da Lei Geral de Proteção de Dados (LGPD) aprovada com antecipação pelo Senado e dependendo apenas da sanção do Presidente para começar a valer, muitas empresas estão tendo que correr atrás do prejuízo e buscar auxílio para se adequarem o mais breve possível.

Em geral, a maioria das organizações esperavam por uma prorrogação da Lei tendo em vista algumas dificuldades para se adaptarem para estas novas diretrizes, principalmente em meio a atual crise que vivemos. O setor de saúde, por exemplo, foi muito impactado pelo evento da Covid-19 e muitos hospitais, laboratórios e centros de saúde não conseguiram realizar as alterações necessárias. Além disso, as pequenas e médias empresas também podem sofrer devido a necessidade de trabalho remoto, dificultando a implementação das regras em atendimento a LGPD.

A realidade é que nunca essa lei foi tão necessária no Brasil como agora, visto a necessidade de ampliar a segurança cibernética devido à adoção do modelo de trabalho remoto ou home office. Independentemente da data em que começará a valer, a LGPD é uma certeza futura e significa um avanço para o país na garantia dos direitos individuais, além de possibilitar um maior desenvolvimento econômico e tecnológico.

As empresas que não cumprirem as normas ditadas poderão ser penalizadas com multas que podem variar entre 2% limitado a R\$ 50 milhões do faturamento total da empresa. Mesmo com o custo alto, segundo pesquisa da Serasa Experian, 85% das empresas brasileiras afirmam ainda não

estar preparadas para garantir os direitos e deveres em relação ao tratamento de dados pessoais exigidos pela LGPD, e um estudo do site Reclame Aqui mostra que 12% das companhias preferem esperar “para ver se a lei vai funcionar” antes de investir em ações. Além das multas e penalidades que poderão ser impostas pela Autoridade Nacional de Proteção de Dados, há também outros gastos como o de despesas de defesa e investigação de proteção de dados; de notificação e monitoramento; relacionados a roubo de dados; e ações regulatórias.

Para as empresas que querem se preparar de forma adequada, uma das maneiras de se protegerem dos riscos e eventual penalidades impostas pela nova legislação é o seguro contra riscos cibernéticos. A modalidade, já amplamente utilizada nos Estados Unidos e na Europa, cobre, entre outras coisas, prejuízos financeiros devido a reclamação de terceiros por violação de privacidade e segurança da informação; perdas do próprio segurado que envolve casos de interrupção de rede devido aos ciberataques ou sabotagem de empregados; interrupção de negócios e lucros cessantes; restauração dos dados digitais que tenham sido destruídos, perdidos, danificados ou alterados durante um comprometimento de rede, cyber extorsão, entre outros.

O primeiro passo para se alcançar um planejamento mais efetivo é que as empresas comecem a enxergar seguros como investimento e não custo. Para se ter uma ideia do investimento, a maioria contrata apólices na faixa de R\$ 20 milhões, mas temos observado que este valor está crescendo, com seguros contratados entre R\$ 30 a R\$ 50 milhões.

Além da proteção sobre o vazamento dos dados, as apólices de seguros cibernéticos cobrem a responsabilidade civil por parte das empresas – que são as responsáveis por proteger as informações – e os prejuízos que essas corporações podem sofrer com a eventual paralisação das suas atividades por conta dos ataques cibernéticos.

Ou seja, o seguro é uma proteção fundamental e a LGPD é uma norma mais que necessária, pois protege usuários e cria um padrão para que todas as instituições possuam as mesmas responsabilidades quanto às informações coletadas. Resta as empresas realizarem um planejamento estratégico adequado e buscarem ajuda especializada para se alinhar a essa nova realidade.

(*) **Ana Albuquerque** é Gerente de linhas financeiras da [Willis Towers Watson](#).