

Rosana Muknicka*

Há menos de 12 meses, somente aqueles que se dedicavam especificamente à área do direito digital e estudos sobre tecnologia discutiam acerca dos impactos das normas de proteção de dados pessoais no Brasil.

Contudo, com a sanção presidencial da Lei 13.709/18, também denominada **Lei Geral de Proteção de Dados (“LGPD”)** e a aprovação pelo Senado Federal da Medida Provisória 869/18, uma verdadeira enxurrada de informações sobre o tema surgiu nos meios de comunicação de massa.

O fato é que, ao contrário do que pensam alguns, esta norma poderá afetar, de forma definitiva e significativa, toda uma cultura de negócios atualmente existente no País.

A LGPD foi inspirada em sua irmã europeia GDPR que, em maio deste ano, comemorou seu aniversário de 1 (um) ano em vigor. Como resultado, o escritório de advocacia DLA Piper, após sofrer na pele as consequências de uma violação de dados, elaborou um relatório esclarecendo que foram reportados aos respectivos órgãos regulatórios europeus 59.000 incidentes em relação à GDPR.

Os incidentes variaram desde pequenas violações, como e-mails enviados para uma pessoa errada até ataques cibernéticos significativos. Segundo este relatório, foram aplicadas 91 multas por violação à GDPR sendo que o órgão francês foi o responsável pela aplicação da multa de valor mais elevado, no importe de 50 milhões de euros para a empresa Google.

Verificando-se os números apontados neste relatório, poder-se-ia chegar à equivocada conclusão de que as sanções aplicadas foram até certo ponto brandas e que, por analogia, os impactos da LGPD no Brasil seriam igualmente suaves. No entanto, importante observar que os países sujeitos à GDPR há anos possuem e respeitam as normas de proteção de dados pessoais existentes.

A GDPR veio, apenas, consolidar o que já era praticado por grande parte dos setores da indústria, comércio e serviços. Esta situação, por certo, não encontra qualquer similaridade com as regras praticadas em nosso território nacional. Não possuímos uma cultura de proteção dos dados pessoais e, ao contrário, somos um dos países que mais encorajamos o compartilhamento de todo tipo de informação mormente nas redes sociais (somos o terceiro país no mundo em número de usuários no Facebook e o segundo no Instagram).

Mas este verdadeiro descaso com os dados pessoais deverá ser repensado o quanto antes pois, enquanto alguns aguardam passivamente o início da vigência da LGPD, órgãos como o Ministério Público do Distrito Federal e Territórios (“MPDFT”) tem ajuizado diversos procedimentos e ações civis públicas com fundamento, inclusive nas regras e princípios trazidos pela LGPD.

Além dos recentes vazamentos de dados ocorridos no Brasil, discutem-se, principalmente, questões relacionadas ao desvio de finalidade na utilização dos dados pessoais, a coleta de dados biométricos e reconhecimento facial, bem como de geolocalização sem o devido consentimento do titular do direito.

Neste cenário encontramos duas figuras: a filial de empresa estrangeira que se sente confortável com a LGPD sob o fundamento de que já observa a GDPR e as empresas nacionais, que mal iniciaram o seu processo de adequação à nova lei.

Ao contrário do que verificamos em grande parte das filiais de empresas europeias no Brasil, não basta a tradução dos documentos elaborados pela matriz sobre a GDPR para se estar em compliance com a LGPD.

Além das diferenças existentes entre as duas legislações, sempre se faz necessário questionar se, na hipótese de um vazamento de dados, quais seriam os passos e procedimentos imediatamente a serem adotados e quem reportaria o fato à autoridade nacional.

Tanto as empresas nacionais quanto estrangeiras deverão, ainda, resolver difíceis questões como a portabilidade, descarte seguro e o direito do titular à exclusão/alteração dos dados pessoais. Temas estes que envolvem custos elevados e que nos levam à constante preocupação da LGPD se tornar o objeto de inúmeras discussões nos tribunais brasileiros, com pedidos de indenizações por danos morais e materiais em razão do descumprimento da norma.

Raras são as empresas que já definiram a figura do encarregado de dados ou que elaboraram seu relatório de impacto. Com a MP 869/18, não há necessidade do encarregado ser pessoa natural com vínculo empregatício ou societário com a empresa. Contudo, as empresas deverão avaliar o risco de incluir terceiros com acesso quase que ilimitado aos seus dados e informações.

Observe-se, ainda, que há grande preocupação com os dados pessoais dos consumidores mas a maioria ignora que realiza o tratamento de dados pessoais dos seus empregados, fornecedores e prestadores de serviços e que, referidos dados, também serão objeto de proteção da LGPD.

Nota-se, portanto, que ainda há um grande caminho a ser percorrido para se observar minimamente as regras trazidas pela LGPD no nosso país.

*Rosana Muknicka, advogada e sócia do escritório Schmidt Valois

Fonte: O Estado de São Paulo, em 11.06.2019.