Na Mídia

20/07/2019 | O Estado de S.Paulo

Os princípios são a garantia da proteção de dados no Brasil

Maria Helena Ortiz Bragaglia

Como é sabido, um dos grandes desafios deste século é o alinhamento entre os avanços tecnológicos e a legislação. As novas relações sociais, comerciais e contratuais que se originam a partir do acesso e do uso maciço da internet demandam um diuturno movimento por parte dos operadores do Direito.

Diante desse cenário, é preciso, cada vez mais, e de forma globalizada, o desenvolvimento e a consolidação de um arcabouço legal que garanta um match perfeito entre a situação prática vivenciada e a efetiva proteção – lato sensu – dos direitos que nascem dessas relações.

Dentre todos os novos desafios relacionados ao tema, a regulamentação da coleta, armazenamento, utilização, tratamento e fluxo de dados pessoais nos parece ser um dos mais relevantes.

Especificamente em relação ao Brasil, a proteção de dados sempre foi tratada de maneira pontual e não estruturada. Recentemente, no entanto, e já não sem tempo, foi sancionada e publicada a Lei 13.709/18 (Lei Geral de Proteção de Dados ou LGPD), a qual dispõe sobre a proteção de dados pessoais.

Além da segurança jurídica que a norma traz, a aprovação da LGPD – que se encontra em vacatio legis – coloca o Brasil em um patamar diferenciado e mais em linha com os demais países que já possuem um marco regulatório, trazendo benefícios à sociedade e à economia do país.

É fato que a existência de um conjunto de normas a respeito do assunto não evitará discussões ou dúvidas a respeito de sua aplicação, alcance e interpretação. Daí a importância dos princípios, os quais funcionam e funcionarão como um referencial geral; ou, em linguagem popular, como um farol a iluminar os caminhos que deverão ser percorridos.

Confira-se, abaixo, de forma pontual e suscinta, os princípios que regem a proteção de dados no Brasil:

Princípios da finalidade e afetação – a informação deve ser armazenada para uma finalidade específica. Em outras palavras, os dados pessoais coletados não podem ser utilizados para finalidades distintas ou

incompatíveis com aquelas que fundamentaram a sua coleta e que tenham sido informadas ao titular.

Princípio da necessidade – não se deve coletar mais informações além das necessárias a se atingir a finalidade almejada. Em outras palavras, trata-se da limitação da coleta e utilização de dados pessoais ao mínimo necessário.

Princípio do livre acesso – a possibilidade de consulta gratuita, pelo titular, aos seus dados pessoais, às modalidades de tratamento e sua integridade, inclusive para que possa exercer o seu direito de retificá-los ou cancelá-los a qualquer tempo.

Princípio da qualidade dos dados – a exatidão dos dados pessoais armazenados, com atualização realizada segundo a periodicidade necessária para o cumprimento da finalidade do seu tratamento.

Princípio da transparência – a informação ao titular sobre a realização do tratamento de seus dados pessoais, com indicação da sua finalidade, categorias de dados tratados, período de conservação destes, e demais informações relevantes.

Princípio da segurança física e lógica – determina o uso, ao responsável pelo tratamento de dados, de medidas técnicas e administrativas proporcionais ao atual estado da tecnologia, à natureza dos dados e às características específicas do tratamento, aptas a proteger os dados pessoais sob sua responsabilidade da destruição, perda, alteração e difusão, acidentais ou ilícitas, ou do acesso não autorizado.

Princípio da boa-fé objetiva – respeito à lealdade e à boa-fé objetiva no tratamento de dados pessoais.

Princípio da responsabilidade – dever de reparação, nos termos da lei, por danos causados aos titulares dos dados pessoais, sejam estes patrimoniais ou morais, individuais ou coletivos.

Princípio da prevenção – o dever do responsável de, além das disposições específicas da LGPD, adotar, sempre que possível, medidas capazes de prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Princípio da não discriminação – a coleta, utilização e tratamento de dados não podem ser mecanismos utilizados para a prática, ou para facilitar a prática de quaisquer atos discriminatórios.

Princípio da responsabilização e prestação de contas (accountability) – as organizações devem implementar medidas técnicas e organizacionais apropriadas a demonstrar que a coleta, utilização e tratamento de dados estão sendo realizadas de acordo com a finalidade e adequação; que todas as normas estão sendo seguidas e, ainda, que os procedimentos adotados, sob o ponto de vista de segurança, são adequados.

Enfim, tendo em vista as mudanças no ambiente tecnológico, não restam dúvidas que os princípios é que permitirão uma atuação integrativa e construtiva, capacitando os operadores do Direito a extrair a melhor solução para o caso concreto.

A mesma premissa se aplica às empresas que atuarão na coleta, armazenamento, utilização, tratamento e fluxo de dados, de tal sorte que, em havendo alguma dúvida sobre eventuais limitações ou riscos decorrentes das atividades, devem e podem se utilizar dos princípios informativos para balizar a sua decisão comercial.

***Maria Helena Ortiz Bragaglia, sócia de Contencioso do Demarest Advogados**