

Por Renato de Oliveira Valença (*)

O Brasil terá até agosto de 2020 para se adaptar à nova Lei Geral de Proteção de Dados (LGPD), sancionada em 2018 e complementada por Medida Provisória editada no final de dezembro (Lei 13.709/2018 e MP 869/2018). Trata-se um importante marco legal que trouxe a total proteção aos dados das pessoas naturais. Estamos falando do nome, telefone, geolocalização, hábitos de consumo e navegação, etnia, digitais, crença religiosa, a cor do cabelo, e de quaisquer outras informações que identifiquem ou tornem alguém identificável.

A LGPD coloca o País em compasso com o que há de mais avançado no mundo ao conferir ao cidadão direitos plenos em relação às informações que a ele pertencem. Os dados passam a ser, de certa forma, encarados como uma “propriedade” pessoal do indivíduo, que passa a ter o direito de obter acesso, conhecimento e controle sobre quem, porque, quais, e sob que circunstâncias suas informações pessoais são utilizadas por empresas e até mesmo por órgãos do governo.

Inspirada no GDPR (*General Data Protection Regulation*) da União Europeia, e pautada no respeito à privacidade, inviolabilidade da intimidade, dignidade e cidadania, a LGPD tem como objetivo principal minimizar os impactos que a utilização de dados pode acarretar na vida e intimidade das pessoas. Para isso, estabeleceu limites e condições sob as quais terceiros poderão “tratar” informações pessoais.

Segundo o novo marco legal, o conceito de “tratamento” abrange a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão e a extração de dados pessoais. Ou seja, abrange tudo. Da coleta ao descarte de dados.

Em diversas hipóteses, as empresas somente poderão tratar dados pessoais mediante o consentimento do titular da informação. O consentimento deve ser uma manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade específica. Se houver intenção ou necessidade de tratamento diferente daquele para o qual houve o consentimento, um novo consentimento da pessoa, para a nova finalidade, deverá ser obtido. Aliás, o consentimento poderá ser revogado a qualquer tempo.

Mais que isso, os titulares de dados pessoais terão o direito de saber se uma determinada empresa trata os seus dados. Poderão ter acesso a essas informações, corrigi-las se estiverem incompletas, inexatas ou desatualizadas. A lei garante ainda que a pessoa possa exigir o bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade e requerer a portabilidade de dados para outro fornecedor. O consumidor poderá, ainda, determinar que seus dados sejam eliminados da base de qualquer empresa.

De acordo com os novos princípios, a quantidade de dados de uma pessoa deverá ser limitada ao mínimo possível, com abrangência não excessiva em relação às finalidades do tratamento. Aos titulares, deverá ser garantida consulta facilitada e clara sobre a forma e duração do tratamento de suas informações. Um outro avanço é que tais dados deverão ser protegidos contra o acesso não autorizado e situações acidentais ou ilícitas.

Como se vê, novos direitos foram criados para os indivíduos. Em contrapartida, passou a existir uma série de obrigações para as organizações, que precisarão rever políticas e se adaptar aos novos preceitos. Afinal, da área de recursos humanos à operação dos negócios, toda a cadeia produtiva empresarial trata o tempo todo com dados pessoais.

A lei entrará em vigor em 14 de agosto de 2020. Até lá, as organizações terão de se preocupar e passar a adotar regras de boas práticas e de governança sobre tratamento de dados, levando em consideração a natureza das informações, escopo, estrutura, escala e volume das operações. E

terão que avaliar a sensibilidade dos dados, probabilidade e gravidade dos riscos, entre outros fatores.

Um dos desafios será a criação de mecanismos de comunicação pelas empresas com os titulares de dados e também com a Autoridade Nacional de Proteção de Dados (ANPD), que acabou de ser criada pela Medida Provisória nº 869/2018.

A ANPD, órgão da administração pública federal ligada à Presidência da República, terá como missão zelar pela proteção dos dados, editar normas e procedimentos, fiscalizar as organizações e aplicar as sanções cabíveis, que poderão chegar a R\$ 50 milhões.

As organizações deverão, ainda, nomear um encarregado de proteção de dados, que será o canal de comunicação da organização perante a ANPD e as pessoas naturais titulares de dados. A Lei 13.709/2018, em seu texto original, estabelecia que o encarregado deveria ser uma pessoa natural. Mas a MP 869 alterou a redação original, excluindo a palavra “natural”. Com isso, abriu a possibilidade de pessoas jurídicas cumprirem esse papel.

Essa abertura poderá significar uma excelente oportunidade para que empresas passem a oferecer esse tipo de assessoria especializada. Cria-se também um nicho para a profissionalização das pessoas físicas que pretendam exercer o cargo de encarregado de proteção de dados. Na Europa, por exemplo, a existência do Data Protection Officer (DPO) nas empresas tem se tornado cada vez mais comum e a atuação desse profissional é bastante abrangente e técnica.

O Brasil terá dois anos para se preparar e adaptar sua economia à LGPD, que representa avanços ao configurar um novo paradigma para as relações empresa/consumidor. Temos, enfim, um marco que traz mais segurança jurídica a uma era na qual, cada vez mais, o mundo se torna digital.

(*) **Renato de Oliveira Valença** é sócio do Peixoto & Cury Advogados, especializado em Direito Societário, Propriedade Intelectual e Publicidade e Comunicação.

Fonte: [O Estado de S. Paulo](#), em 11.01.2019.