Projeto de Lei de proteção dos dados pessoais é aprovado no Senado

Após já ter sido aprovado na Câmara, projeto ainda precisa ser sancionado pelo presidente da República

O plenário do Senado aprovou na última terça-feira, 10/7, o **Projeto de Lei número 53 ,** da Câmara, que disciplina a proteção dos dados pessoais e define as situações em que estes podem ser coletados e tratados tanto por empresas quanto pelo Poder Público. O texto foi aprovado nos termos do conteúdo votado na Câmara dos Deputados no fim de maio, mas ainda precisa ser sancionado pelo presidente Michel Temer.

O texto disciplina a forma como as informações são coletadas e tratadas, especialmente em meios digitais, como dados pessoais de cadastro ou até mesmo textos e fotos publicadas em redes sociais. A proposta foi mantida na semana anterior pela Comissão de Assuntos Econômicos (CAE), conservando o conteúdo da Câmara e indicando regime de urgência para votação na casa. A urgência foi apresentada em plenário, mas não chegou a ser apreciada.

Entenda o projeto

O PLC 53 considera dados pessoais a informação relacionada a uma pessoa que seja “identificada” ou “identificável”. Ou seja, o projeto de lei regula também aquele dado que, sozinho, não revela a quem estaria relacionado (um endereço, por exemplo) mas que, processado juntamente com outros, poderia indicar de quem se trata (o endereço combinado com a idade, por exemplo).

Foi criada uma categoria especial, denominada dados “sensíveis”, que abrange registros de raça, opiniões políticas, crenças, condição de saúde e características genéticas. O uso desses registros fica mais restrito, já que traz riscos de discriminação e outros prejuízos à pessoa.

Também há parâmetros diferenciados para processamento de informações de crianças, como a exigência de consentimento dos pais e a proibição de condicionar o fornecimento de registros à participação em aplicações (como redes sociais e jogos eletrônicos).

O projeto de lei abrange as operações de tratamento realizadas no Brasil ou a partir de coleta de dados feita no país. A norma também vale para empresas ou entes que ofertem bens e serviços ou tratem informações de pessoas que estão aqui. Assim, por exemplo, por mais que o Facebook recolha registros de brasileiros e faça o tratamento em servidores nos Estados Unidos, ele teria de respeitar as regras. Também é permitida a transferência internacional de dados (como no exemplo citado), desde que o país de destino tenha nível de proteção compatível com a lei ou quando a empresa responsável pelo tratamento comprovar que garante as mesmas condições exigidas pela norma por instrumentos como contratos ou normas corporativas.

Ficaram de fora das obrigações o tratamento para fins pessoais, jornalísticos e artísticos. Também não são cobertos o processamento de informações em atividades de segurança nacional, segurança pública e repressão a infrações. O texto indica que esses temas devem ser tratados em uma lei específica. O Poder Público ganhou também a possibilidade de tratar dados sem consentimento das pessoas, em determinadas situações, como na execução de políticas públicas. Para isso, o órgão deve informar em seu site em que hipótese o processamento de dados é realizado, sua finalidade e quais são os procedimentos adotados. Essas regras especiais se aplicam também aos cartórios.

Obrigações e direitos

Para coletar e tratar um dado, uma empresa ou ente precisa solicitar o consentimento do titular, que deve ser livre e informado. Essa autorização deve ser solicitada de forma clara, em cláusula específica, e não de maneira genérica. Caso uma empresa colete um dado para uma coisa e mude sua finalidade, deve obter novo consentimento. A permissão dada por alguém, entretanto, pode ser revogada se o titular assim o desejar.

O projeto prevê, contudo, algumas situações em que este não é necessário, como a proteção da vida, o cumprimento de obrigação legal e procedimento de saúde. A exceção mais polêmica é chamada de “legítimo interesse”, que na prática permite a uma empresa coletar um dado para um propósito e usá-lo para outro, desde que para “finalidades legítimas” e a “partir de situações concretas”. Nesse caso, somente os dados “estritamente necessários” podem ser

manejados.

Outra obrigação das empresas incluída no relatório do deputado Orlando Silva (PCdoB-SP) é a garantia da segurança dos dados, impedindo acessos não autorizados e qualquer forma de vazamento. Caso haja algum incidente de segurança que possa acarretar dano ao titular da informação, a empresa é obrigada a comunicar à pessoa e ao órgão competente.

A redação prevê uma série de direitos ao titular, que pode solicitar acesso às informações que uma empresa tem dele - incluindo a finalidade, a forma e a duração do tratamento - e se houve uso compartilhado com algum outro ente e com qual finalidade. Também é possível requisitar a correção de um dado incompleto, a eliminação de registros desnecessários ou excessivos e a portabilidade para outro provedor de serviço. Ou seja, o usuário de uma conta de e-mail pode ter todas as suas mensagens, caso deseje abrir conta em outro serviço deste tipo. O titular também pode solicitar a revisão de uma decisão automatizada baseada em seus dados, como uma classificação para obtenção de crédito, por exemplo.

Fiscalização e órgão regulador

O relatório de Silva propõe a criação da Autoridade Nacional de Proteção de Dados, que ficará responsável pela edição de normas complementares e pela fiscalização das obrigações previstas na lei. Essa autoridade terá poder, por exemplo, para exigir relatórios de impacto à privacidade de uma empresa, documento que deve identificar como o processamento é realizado, as medidas de segurança e as ações para reduzir riscos. Ou seja, se o órgão suspeitar que em alguma empresa há risco de problemas no tratamento dos dados, o relatório reúne informações necessárias para uma primeira apuração. Pode também fazer uma auditoria, em que se verifique no local da empresa se o manejo dos dados está sendo realizado corretamente.

Se constatar alguma irregularidade em qualquer atividade de tratamento, a autoridade pode aplicar uma série de sanções, entre as quais está prevista multa de até 2% do faturamento da empresa envolvida, com limite de R$ 50 milhões, o bloqueio ou eliminação dos dados tratados de maneira irregular e a suspensão ou proibição do banco de dados ou da atividade de tratamento. O substitutivo também institui o Conselho Nacional de Proteção de Dados, formado por 23 representantes do Poder Público, da sociedade civil, de empresas e de instituições científicas e tecnológicas. O colegiado tem como atribuições propor diretrizes estratégicas sobre o tema e auxiliar a autoridade nacional.

Fonte: **CNSeg** , em 11.07.2018.