Instituto Brasileiro de Defesa do Consumidor

Nota técnica sobre aprovação da Lei de Dados Pessoais na Câmara dos Deputados em 29 de maio de 2018

Autores: Rafael A. F. Zanatta, Barbara Simão, Juliana Oms e Henrique Meng

Introdução

As discussões em torno de uma Lei de Proteção de Dados Pessoais chegaram ao fim na Câmara dos Deputados na noite de terça-feira (29/05). De forma consensual, o Plenário aprovou o PL 4060/2012 na forma do substitutivo do deputado Orlando Silva (PCdoB/SP).

O substitutivo é fruto do trabalho de dois anos da Comissão Especial de Tratamento e Proteção de Dados Pessoais, formada após o apensamento de dois projetos de lei: o PL 4060/12, de autoria do deputado Milton Monti (PR/SP), e o PL 5276/16, de autoria da ex-Presidenta Dilma Rousseff.

A Comissão Especial realizou 11 audiências públicas desde sua criação em agosto de 2016. Em outubro de 2016, os trabalhos foram iniciados após designação de membros pelo Presidente da Câmara, Rodrigo Maia.

O Instituto Brasileiro de Defesa do Consumidor participou de quatro audiências públicas da Comissão Especial: em dezembro de 2016 (direitos dos cidadãos e funcionamento da autoridade de proteção de dados), maio de 2017 (responsabilidade objetiva e solidária em casos de danos), maio de 2017 (seminário internacional sobre proteção de dados em perspectiva comparada) e maio de 2018 (modelo regulatório para proteção de dados pessoais).

Nos últimos meses, o Idec trabalhou em conjunto com entidades da Coalizão Direitos na Rede no envio de contribuições ao substitutivo preparado pelo relator

Orlando Silva (PCdoB/SP). Em abril, o Instituto havia defendido a priorização da lei de dados pessoais antes da votação da reforma do Cadastro Positivo. Para o Idec, "com uma legislação forte sobre dados pessoais e normas executáveis por uma autoridade distinta do Banco Central, o cadastro positivo geraria menos riscos coletivos em sua tentativa de democratização das finanças".

A aprovação da Lei de Dados Pessoais na Câmara avança no controle de riscos coletivos e se aproxima do sistema adotado na União Europeia, especialmente com a entrada em vigor do "Regulamento Geral de Proteção de Dados" (RGDP). Desde o "escândalo Facebook", em março de 2018, cresceu a consciência pública sobre a necessidade de direitos básicos e maior controle sobre o modo como dados pessoais são utilizados e compartilhados com terceiros.

1. O que o Idec defendeu e o que foi aprovado?

Desde 2011, o Idec tem lutado para aprovação de uma Lei Geral de Proteção de Dados Pessoais no Brasil. O Instituto produziu pesquisas, matérias, eventos, oficinas e textos de posição para o Congresso.

Em agosto de 2017, o Idec apresentou, no Seminário de Proteção de Dados Pessoais do Comitê Gestor da Internet, **treze pontos** fundamentais de uma legislação voltada aos cidadãos. Analisamos, a seguir, de que modo a Lei de Dados Pessoais aprovada na Câmara dos Deputados se adequa a essas demandas.

(i) conceito de dados pessoais deve ser expansivo: o projeto aprovado na Câmara afirma que dado pessoal é qualquer "informação relacionada à pessoa natural identificada ou identificável" (art. 5º, I). Esse conceito permite que metadados (dados de utilização de dispositivos), geolocalização, endereço I.P. e outros sejam considerados como dados pessoais.

(ii) proteção especial a dados sensíveis, incluindo dados de saúde, informações genéticas e biométricas: uma das disputas recentes se dava sobre a inclusão de dados biométricos como dados sensíveis. No texto aprovado na Câmara, os dados sensíveis incluem dados genéticos e biométricos (art. 5º, II). Também há proteção especial

para informações de origem racial, convicções religiosas, filiação a sindicatos ou organizações políticas e vida sexual.

(iii) se dados anonimizados puderem ser revertidos com esforços técnicos razoáveis, eles devem ser considerados dados pessoais: os "dados anonimizados" são aqueles em que um titular (uma pessoa) deixa de ser identificado por meio de processos técnicos. O artigo 12 do projeto afirma que os dados anonimizados serão considerados dados pessoais se os esforços de anonimização puderem ser revertidos "com esforços razoáveis".

(vi) dados utilizados para formação de "perfil comportamental" (profiling) merecem proteção especial para coibir práticas discriminatórias: o projeto da Câmara afirma no art. 12, §2º, que "poderão ser igualmente considerados como dados pessoais aqueles utilizados para a formação de perfil comportamental de uma determinada pessoa natural, se identificada". O projeto também prevê, no art. 20, que o titular tem direito a solicitar revisão de decisões "tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses". Caso a pessoa não consiga analisar os procedimentos de decisão automatizada em razão de segredo industrial, a autoridade de proteção de dados "poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizados de dados pessoais" (art. 20, § 2º).

(v) a lei deve ter como fundamentos o "consentimento inequívoco" e a "autodeterminação informativa": O projeto de lei coloca em seu art. 2º que a proteção de dados pessoais tem como fundamento a autodeterminação informativa (direito de as pessoas conhecerem e controlarem os fluxos de informação gerados por elas próprias). Na definição de "consentimento" no art. 5º, XII, há qualificação de que o aceite por parte do titular dos dados deve ser livre, informado e inequívoco.

(vi) deve-se vedar autorizações genéricas para coleta de dados pessoais e tornar obrigatória a explicação clara da finalidade da coleta, tratamento e transmissão: o artigo 6º do projeto cria um conjunto de princípios para tratamento de dados, incluindo o "princípio da finalidade" (art. 6º, I), que diz que a utilização de dados

pessoais deve ter "propósitos legítimos, específicos, explícitos e informados ao titular". Termos de uso gerais também são vedados pelo "princípio da necessidade e minimização" (art. 6º, III), que diz que o tratamento "deve se limitar ao mínimo necessário para a realização das suas finalidades, abrangendo dados pertinentes, proporcionais e não excessivos". Além disso, a lei afirma que são nulas de pleno direito as "autorizações genéricas para o tratamento de dados pessoais" (art. 8º, § 4º).

(vii) a autoridade de proteção de dados pessoais deve ter caráter técnico e capacidade de monitoramento das práticas da administração pública e do setor privado: a lei aprovada na Câmara cria uma Autoridade Nacional de Proteção de Dados, submetida a regime autárquico e vinculada ao Ministério da Justiça (art. 55), caracterizada por "independência administrativa, ausência de subordinação hierárquica, mandato fixo e estabilidade de seus dirigentes e autonomia financeira" (art. 55. § 3º). A Autoridade será gerida por três conselheiros que formam o Conselho Diretor (art. 55, § 2º), nomeados por decreto. Abaixo do Conselho Diretor, a Autoridade terá o Conselho Nacional de Proteção de Dados Pessoais (art. 58), composto por 23 representantes, aos moldes do Comitê Gestor da Internet. O projeto prevê a participação de quatro membros de instituições científicas e tecnológicas (art. 58, VIII) e quatro membros da sociedade civil "com atuação comprovada em proteção de dados pessoais" (art. 58, II).

(viii) em caso de coleta de dados sem consentimento (por legítimo interesse), a autoridade deve ter o poder de exigir relatório de impacto à proteção de dados pessoais: o texto aprovado na Câmara define "relatório de impacto à proteção de dados pessoais" (RIPDP) como a "documentação do responsável que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco" (art. 5º, XVII). No artigo que trata do legítimo interesse (art. 10), o texto de lei diz que o órgão competente pode solicitar ao responsável um RIPDP quanto o "tratamento tiver como fundamento o seu interesse legítimo" (art. 10, § 3º). No artigo 38, esse poder do órgão competente é reafirmado, inclusive em casos de coleta de dados sensíveis. O texto diz que o relatório deve

conter, no mínimo, descrição dos tipos de dados coletados, a metodologia utilizada para sua coleta e para garantia da segurança das informações, bem como análise do responsável com relação às medidas, salvaguardas e mecanismos de mitigação de riscos adotados (art. 38, parágrafo único).

(ix) a coleta e o tratamento de dados pessoais devem obedecer ao princípio da minimização: o "princípio da minimização" foi adensado ao "princípio da necessidade". Empresas precisam coletar o mínimo possível e há vedação para termos de uso genéricos, conforme explicado acima.

(x) os cidadãos possuem direitos básicos de acessar, retificar ou revogar o consentimento de forma gratuita e facilitada, bem como realizar a portabilidade de seus dados pessoais: o artigo 18 cria os direitos básicos dos titulares de dados pessoais, incluindo o direito de acesso, de correção de dados incompletos, de eliminação de dados e de portabilidade de dados, "mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação" (art. 18, IV). A questão de como a portabilidade vai ser executa fica para depois, com regulamentação criada pela Autoridade de Proteção de Dados Pessoais.

(xi) A responsabilidade civil no caso de reparação de danos causados aos titulares de dados, na cadeia de processamento, deve ser objetiva e solidária: um dos pontos mais polêmicos da discussão, a solução encontrada pelo projeto da Câmara é a criação de um modelo sofisticado, separando os casos em que há relação de consumo (exemplo: utilização de um aplicativo por um consumidor) e os casos em que não há (exemplo: uso de dados entre empresas). O projeto prevê duas figuras jurídicas: a do "responsável" (quem coleta os dados e supervisiona) e do "operador" (quem é contratado para desempenhar uma tarefa). O projeto prevê que, a fim de assegurar a efetiva indenização ao titular dos dados, o operador responde solidariamente pelos danos causados pelo tratamento quando "descumprir as obrigações da legislação de dados" ou quando "não tiver seguindo as instruções lícitas do responsável" (art. 42, I). O projeto prevê excludentes de responsabilidade no art. 43 (exemplo: dano decorrente de culpa exclusiva do titular). O tratamento de dados também é considerado irregular quando "não fornecer a segurança que o titular dele pode

esperar" (art. 44). Por fim, o art. 45 prevê que, quando há relação de consumo, as hipóteses de violação "permanecem sujeitas às regras de responsabilidade" previstas no Código de Defesa do Consumidor. Nesse caso, a responsabilidade é objetiva, como defendido pelo Idec.

(xii) a indústria deve implementar processos de privacidade por tecnologia na concepção de técnicas de coleta e tratamento de dados pessoais: apesar de não existir uma norma específica sobre "privacy by design", o projeto de lei menciona o "princípio da prevenção" no art. 6º e estimula que o setor privado elabore melhores práticas para proteção de dados pessoais. Além da determinação de um encarregado por dados pessoais (art. 41), há um capítulo de segurança e boas práticas que pede que os agentes adotem "medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais" (art. 46), com enfoque em segurança e sigilo dos dados.

(xiii) a "avaliação de impacto à proteção de dados pessoais" deve ser obrigatória no caso de tratamento que provavelmente resulte em alto risco aos cidadãos, a partir de critérios objetivos definidos pela autoridade de proteção de dados: esse último ponto não foi contemplado pela legislação. O projeto aprovado na Câmara prevê relatórios de impacto à proteção de dados pessoais e dá poderes à autoridade para exigi-los, mas não determina casos objetivos onde eles são obrigatórios, como no caso do Regulamento Europeu (exemplo: coleta de dados em áreas geográficas abertas ou criação de perfis comportamentais com dados sensíveis).

2. Avaliação final: uma lei forte que merece aprovação

Como visto, dos treze pontos fundamentais defendidos pelo Idec e pela Coalizão Direitos na Rede, o projeto na Câmara contempla doze. Trata-se de um projeto bastante robusto da perspectiva da garantia de direitos básicos aos cidadãos e adequação do sistema jurídico brasileiro a uma economia de dados moderna, capaz de aliar segurança jurídica e garantia de direitos fundamentais.

O fato de o relator do projeto ter mencionado o papel da sociedade civil, dos acadêmicos e das empresas na construção da versão final da lei também fortalece a visão de que a criação dessas regras seguiu um processo multissetorial, como exigido

pelo Marco Civil da Internet (Lei 12.965/14). Com a aprovação da lei de dados pessoais, o Brasil pode completar o "tripé regulatório" para a cidadania online: uma Lei de Acesso à Informação, um Marco Civil da Internet e uma Lei Geral de Proteção de Dados Pessoais.

A solução de todos os males não está nesse tripé, mas a afirmação desses direitos é um passo importante para equilibrar nosso impulso por inovação e a garantia de direitos fundamentais. Afinal de contas, como defendemos no Instituto, nossos dados não são apenas mercadoria. É hora de pensar nesses direitos em uma dimensão coletiva, garantir a autonomia dos indivíduos e evitar aspectos discriminatórios em uma sociedade cada vez mais dependente de computadores, algoritmos e bases de dados.