MANIFESTO SOBRE A FUTURA LEI DE PROTEÇÃO DE DADOS PESSOAIS

SETEMBRO DE 2016

É inquestionável o papel que a Internet tem na sociedade como viabilizadora de inclusão social, indutora de crescimento econômico, inovação e avanço tecnológico. Especialistas preveem que o tratamento e a monetização de dados gerarão cerca de US$ 1,6 trilhão de valor agregado nos próximos quatro anos.

Neste contexto, a proteção de dados pessoais é um dos grandes desafios da atualidade. O Brasil tem a oportunidade de conceber uma Lei de Proteção de Dados Pessoais moderna e balanceada, que proteja os direitos do cidadão e que seja impulsionadora do desenvolvimento tecnológico e de modelos de negócios inovadores.

As entidades que subscrevem este manifesto entendem que a futura lei de proteção de dados pessoais deve contemplar os aspectos detalhados a seguir.

DADO PESSOAL

Devem ficar sujeitos à lei somente os dados que inequivocamente possam ser utilizados para identificar a pessoa natural, podendo assim afetar a sua privacidade, devendo ser excluídos desta definição todos os demais.

Um conceito amplo de dado pessoal pode inibir o desenvolvimento da economia e inovação baseada em dados, na medida em que os tratamentos englobam dados que são meramente relacionados a pessoas naturais ou identificação eventual quando combinados com outros dados pessoais. Uma conceituação ampla tornaria praticamente todos os dados produzidos pela atividade humana sujeitos à Lei, ainda que não possam ser utilizados para identificar inequivocamente o titular.

Recomenda-se a seguinte definição de **dado pessoal: qualquer dado que identifique de forma exata e precisa uma pessoa natural**.

DADOS PESSOAIS SENSÍVEIS

Recomenda-se que seja adotada uma definição de dados sensíveis taxativa, evitando-se definições abertas e genéricas, a exemplo do que se dá em outros países, em razão de sua especialidade e das diversas restrições impostas à sua coleta e tratamento.

Em geral, não se configuram como dados de saúde os dados gerados por aplicativos de estilo de vida e dispositivos medidores, não requerendo, portanto, proteção especial. Por outro lado, direito à manifestação pública a respeito de convicções religiosas, opiniões políticas, ou filiação a sindicatos não deve ser cerceado. Assim sendo a futura lei de proteção de dados deve reconhecer e respeitar a expressão de tais convicções ou filiações, quando forem espontânea e livremente fornecidas pelos titulares, como manifestação de pensamento, consciência ou crença, e que constituem a base da liberdade de expressão e do exercício pleno da cidadania.

Portanto, recomenda-se a seguinte definição de **dados sensíveis: dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados relacionados a condição médica do titular, genéticos e referentes à orientação afetiva e de gênero.**

Neste sentido, recomenda-se que o tratamento de dados pessoais sensíveis, voluntariamente disponibilizados por seus titulares, prescinda de consentimento diferenciado, como se segue: **Os dados pessoais sensíveis que sejam voluntariamente disponibilizados por seus titulares como manifestação de sua liberdade de expressão, consciência ou crença, poderão ser tratados como dados pessoais.**

DADOS ANÔNIMOS

Os dados não relacionados a uma pessoa natural específica são a espinha dorsal do modelo da economia impulsionada por dados, que hoje representa um acelerador do desenvolvimento econômico e da inovação tecnológica. Não devem estar sujeitas à aplicação da Lei dados pessoais que tenham sido anonimizados ou que de qualquer outra forma não possam identificar a pessoa natural. Recomenda-se a seguinte definição de **dados anônimos: dados relativos a um titular que não seja identificado.**

CONSENTIMENTO

A adoção do consentimento livre e inequívoco, em oposição ao consentimento expresso estabelecido em outros diplomas legais, viabiliza o tratamento de dados no ambiente digital conectado, permite a contínua inovação baseada em dados e assegura o nível de proteção adequado ao titular.

O **consentimento inequívoco**, inserido como regra geral para a manifestação do consentimento, é entendido como **uma declaração do titular** que visa a proteger seus direitos e se compatibiliza com o dinamismo da era da Internet, podendo ser **expressa por escrito, por meios eletrônicos, declarações orais, configurações técnicas** para o processamento de dados e informações pessoais, **ou qualquer outra forma** de expressar a aceitação do titular quanto ao processamento e tratamento dos seus dados pessoais.

Ressalte-se a necessidade de harmonizar a Lei 12.965/2014, Marco Civil da Internet, às disposições da futura Lei de Proteção de Dados Pessoais.

DO INTERESSE LEGÍTIMO

O reconhecimento do legitimo interesse implica em que dados podem ser regularmente tratados, sem a necessidade de obtenção de consentimento, sempre que o responsável tiver interesse em tal tratamento, mediante balanceamento com os interesses, direitos e liberdades fundamentais do titular dos dados e a necessidade do tratamento do dado.

A importância do interesse legítimo é evidenciada ante a constatação de que o conceito tradicional de consentimento não lida adequamente com o tratamento de dados em larga escala ("big data") e com o cenário de novos dispositivos conectados.

RESPONSABILIDADE CIVIL

A responsabilização das empresas que tratam dados e prestam serviço ao usuário em relação aos dados pessoais deve se dar no tocante (i) ao respeito aos **direitos e liberdades fundamentais** do titular, (ii) ao **tratamento dos dados** no âmbito do consentimento, do legítimo interesse, ou nas demais hipóteses previstas em lei, e (iii) ao **dever de guarda** dos dados tratados.

No caso de descumprimento de seus deveres, **a empresa que** tratou os dados responderá **pelos danos causados** ao titular dos dados estritamente no âmbito de sua atuação dentro da cadeia de tratamento, devendo ser apuradas as respectivas responsabilidades de cada uma das demais empresas especializadas por ela contratadas.

Por sua vez, a responsabilização das empresas subcontratadas na cadeia de tratamento deve se dar no tocante (i) aos **termos e condições pelos quais foram contratadas** e (ii) ao **dever de guarda** dos dados a serem tratados e os respectivos resultados do tratamento, **sem a necessidade de regulação *ex ante*** por parte de eventual Órgão Competente.

Veja-se que, por serem pessoas jurídicas diversas e independentes, as empresas não poderão exercer controle sobre as atividades umas das outras e, portanto, não é razoável atribuir-se responsabilidade solidária entre elas por atos sobre os quais não tem poder de supervisão que lhes permita controlar e evitar os prejuízos que serão obrigadas a reparar. Convém citar o exemplo do Cadastro Positivo, em que a responsabilidade objetiva e solidária entre fontes, consulentes e bancos de dados, tem representado um importante entrave para a implementação exatamente em razão do argumento acima exposto.

Ressalte-se que as empresas que compõem a cadeia de empresas subcontratadas pela empresa que trata os dados e presta serviço para o usuário, podem estar no Brasil ou em qualquer outro lugar do mundo.

Sugere-se, portanto, que as empresas cedentes (empresas que coletam dados e prestam serviço ao usuário) e cessionárias (empresas subcontratadas na cadeia de tratamento) respondam dentro dos limites de sua atuação pelos danos decorrentes na cadeia de tratamento de dados, independentemente do local onde estes se localizem, devendo ser apuradas as respectivas responsabilidades, cabendo (i) ao cedente, a responsabilidade pela integridade dos dados pessoais transmitidos tais como coletados e pela comunicação de eventuais alterações nos dados ou no consentimento ao cessionário; (ii) ao cessionário, a integridade dos dados pessoais tais como transmitidos pelo cedente, pelo seu tratamento em conformidade com as hipóteses legais e pela integridade dos dados de acordo com posteriores comunicações do cedente.

Transferência Internacional de Dados

O fluxo internacional de informações é uma importante fonte de valor econômico e social, sendo que um dos grandes benefícios da sociedade digital está justamente nas economias de escala advindas desse ecossistema. A experiência recente demonstra que as medidas adotadas pelas empresas para garantir a segurança da transferência internacional de dados são tão ou mais eficazes para proteger os dados e bem mais ágeis no acompanhamento da inovação tecnológica, do que sistemas regulatórios baseados na avaliação *ex ante* da adequação de sistemas regulatórios estrangeiros. **Assim, as empresas são incumbidas por zelar pela integridade dos dados e serão responsabilizadas caso ocorra a transferência para empresas que não adotem política de proteção adequada, sem a necessidade de regulação *ex ante*** por parte de um Órgão Competente.

Órgão Regulador Independente

É fundamental a criação de uma autoridade federal independente para interpretar, fiscalizar e fazer cumprir a futura norma sobre proteção de dados pessoais. Internacionalmente, quase todos os países que promulgaram leis de proteção de dados pessoais criaram um órgão nacional específico e independente com essas competências.

As vantagens de um modelo de autoridade federal independente estão na consistência das interpretações, a especialização técnico-jurídica sobre o tema, a certeza regulatória e a independência necessária para atuar de modo eficaz e sopesar todos os direitos e interesses em jogo. Ressalve-se, porém, que o orçamento operacional do órgão deve ser autônomo, sem incluir eventuais multas impostas em decorrência de violações à lei, pois do contrário haveria um claro conflito de interesses e incentivo a distorções.

Sanções e Proporcionalidade

As sanções previstas na futura lei devem ser proporcionais à natureza das violações de direito e dos danos efetivamente causados. Sanções que suspendem ou proíbem o tratamento de dados, ainda que por tempo determinado, podem acarretar o encerramento de atividades empresariais, abrindo espaço para possível violação dos direitos fundamentais dos titulares, como liberdade de expressão e comunicação, representando um forte fator de insegurança jurídica e de desestímulo a investimentos e à prestação de serviços no Brasil.

Vacatio Legis

Em razão da complexidade do seu objeto, leis de proteção de dados afetam de forma ampla (a) o setor privado, que se adapta às novas regras, (b) a Administração Pública, que se organiza para desempenhar novas funções, e (c) o poder judiciário, que empreende a exegese da lei. A experiência Internacional, em especial a Europeia, demonstra que se faz mister um período de transição e adaptação, tendo em vista o novidadismo. Assim sendo, sugere-**se que a futura lei entre em vigor após 3 (três) anos, contados a partir da data da sua sanção.**

LEGITIMIDADE DA COLETA E TRATAMENTO ANTERIORES À LEI

O direito brasileiro adota como regra geral a irretroatividade dos efeitos da nova lei, protegendo o ato jurídico perfeito. Os novos requisitos a serem trazidos pela futura lei não invalidam os dados coletados e tratados sob a égide da legislação vigente à época. Condiciona-se, porém, novos tratamentos, bem como os direitos de acesso e retificação, ao disposto na futura lei. Sugere-se, portanto, que **os dados pessoais armazenados pelos responsáveis em conformidade com a legislação vigente à época de sua coleta não estarão sujeitos à obtenção do consentimento dos seus titulares, aplicando-se às subsequentes operações de seu tratamento, contudo, as demais disposições desta lei.**