

Contribuição à Consulta Pública sobre o Ante-Projeto de Lei de Proteção de Dados Pessoais instituída pelo Ministério da Justiça

I – Introdução

A PROTESTE – Associação de Consumidores apoia fortemente a iniciativa do Ministério da Justiça de propor uma lei de proteção de dados pessoais.

Entendemos que o projeto de lei adotou premissa de grande importância, determinando que o foco da proteção dos dados pessoais deve se dar com base na garantia da titularidade dos dados sempre pelo cidadão ou consumidor e, como consequência, estabelecendo a regra da obrigatoriedade de seu consentimento expresso, informado e limitado para a coleta e tratamento de dados, impedindo presunções de autorização pelo silêncio.

Ainda que a proposta de lei não se dirija apenas às relações estabelecidas nos meios digitais, o certo é que o enorme crescimento da utilização da internet para a comercialização de produtos e serviços, para a prestação de serviços públicos e para a intensa comunicação por redes sociais, blogs etc..., somado ao desenvolvimento da tecnologia para coleta e tratamento de dados de forma massiva e arbitrária, com vistas à identificação de mercados e controle político, faz-se urgente uma atuação efetiva do Estado para a proteção dos cidadãos já há alguns anos, que estão sujeitos às regras dos mercados e arbitrariamente adotadas por governos e órgãos públicos, como os órgãos de investigação, por exemplo.

Ainda que o Brasil esteja atrasado na missão de instituir ferramentas que habilitem os cidadãos para um grau razoável e possível de controle a respeito da utilização de seus dados, poderemos usar este fato como vantagem, apropriando-nos das experiências de outros países para editar uma lei mais atual e compatível com o mercado e, por isso, mais efetiva.

Esperamos que os trâmites seguintes à entrega das contribuições pela sociedade sejam céleres, pois entendemos que uma Lei de Proteção de Dados Pessoais tem papel complementar com o Código de Defesa do

Consumidor e com o Marco Civil da Internet, fortalecendo os cidadãos e consumidores nas relações com empresas e governos.

II – A necessidade de se instituir por meio da lei a Autoridade Competente com poderes fiscalizatório e sancionatório

Sendo assim, a primeira contribuição da PROTESTE vai no sentido de que se inclua na lei diretrizes para a criação de órgão de natureza pública com competência para regulamentar, fiscalizar e aplicar sanções nos casos de descumprimento da lei.

Inclusive porque o APL faz menção repetidas vezes a um órgão competente e suas atribuições, mas frustra as expectativas, pois não trouxe nem mesmo linhas gerais a fim de viabilizar a instituição deste órgão.

A PROTESTE realizou, em março deste ano com o apoio do Comitê Gestor da Internet no Brasil, o Seminário Marco Civil da Internet: Neutralidade e Proteção de Dados Pessoais, no qual representante da Agência Espanhola de Proteção de Dados (existente desde 1993) – Luis Antonio Salvador Carrasco¹ – proferiu palestra informando a extrema importância e o papel preponderante de um órgão com funções reguladoras e fiscalizadoras para por freio aos abusos perpetrados pelos agentes econômicos na coleta e tratamento de dados, tendo sido impostas multas com valores EU\$ 20 milhões por ano, bem como destruição de bancos de dados no ato de fiscalização.

Destaque-se que a agência espanhola tem competência inclusive para fiscalizar arquivos da administração pública como a Polícia, Poder Judiciário, ainda que no caso dos órgãos públicos não haja previsão de sanção, mas a expedição de atos administrativos com a determinação de cumprimento da lei.

Trata-se de organismo com autonomia política e administrativa do Poder Executivo. A agência tem um único diretor com mandato a cada 4 anos, sem possibilidade de recondução, escolhido por uma comissão formada por

¹ . <https://www.youtube.com/watch?v=cwQD0QpLSW4>

² <http://www.internetlab.org.br/pt/internetlab-reporta/internetlab-reporta->

membros do Senado, do Congresso, do Judiciário, dos advogados entre outros representantes da sociedade.

O financiamento da agência, com custo de 13 milhões de euros em 2013, se dá por intermédio da arrecadação de multas. Em 2013 foram arrecadados 22 milhões de euros em multas pela agência. O excedente entre o custo de manutenção da agência e o total do valor arrecadado é direcionado para a Fazenda Pública.

Ainda que em caráter ilustrativo, entendemos que o modelo adotado pela Espanha pode servir de parâmetro para que a lei brasileira a ser instituída já estabeleça sobre a criação de uma autoridade com competência para regular, fiscalizar e aplicar sanções.

Caso contrário, considerando-se o grau de vulnerabilidade dos cidadãos na relação que mantêm com empresas e governos quanto ao controle de seus dados, teremos pouca efetividade.

II – Dados Sensíveis

O art. 5º, inc. III, traz a seguinte definição do que sejam dados sensíveis:

“dados pessoais que revelem a origem racial ou étnica, as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, bem como dados genéticos”

A finalidade clara, legítima e justificada da lei ao definir o que sejam dados sensíveis é evitar tratamento discriminatório aos cidadãos.

Sendo assim, entendemos ser importante incluir mais dois tipos de dados na definição em questão, quais sejam: a) dados relativos à condição socioeconômica e b) e dados biométricos.

Isto porque estes dados revelam aspectos muito sensíveis da privacidade, com alto potencial de discriminações ilícitas no momento de contratação de produtos e serviços.

Sendo assim, propomos a seguinte redação ao inc. III:

dados sensíveis: dados pessoais que revelem a origem racial ou étnica, as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação a

sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, **às condições socioeconômicas**, bem como dados genéticos **e dados biométricos, observando-se quanto a esse último o disposto no artigo 13, §2º.**

Tendo em vista o mesmo fundamento e considerando o princípio da necessidade expresso no inc. III, do art. 6º, propomos que ao § 1º, do art. 13, se dê a seguinte redação:

§ 1º A realização de determinadas modalidades de tratamento de dados pessoais sensíveis poderá ser condicionada à autorização prévia de órgão competente, nos termos do regulamento, **levando-se em consideração, dentre outros princípios, o quanto disposto no artigo 6º, inciso III.**

III – Dados Anônimos

O APL no art. 1º estabelece que o âmbito de aplicação da lei é a proteção de dados pessoais, com o objetivo de proteger os direitos fundamentais de liberdade, intimidade e privacidade da pessoa natural.

O art. 5º, inc. I, define o que sejam dados pessoais, enquanto o inc. IV define o que sejam dados anônimos, do que se pode concluir que a lei não teria incidência sobre os dados anônimos.

Contudo, a tecnologia hoje já permite que dados anonimizados possam ser reidentificados, fato este indicativo de que também os dados anônimos deveriam estar contemplados pela lei de proteção de dados pessoais.

Para reforçar este entendimento, oportuna a transcrição dos comentários de Jamila Venturini e Luiz Fernando Moncau, ambos do Centro de Tecnologia e Sociedade da FGV do Rio de Janeiro publicados no site do InternetLab²:

Afinal, dados anônimos estão mesmo fora da área de aplicação do anteprojeto de lei?

Comentário: Jamila Venturini e Luiz Fernando Moncau (pesquisadora e gestor do Centro de Tecnologia e Sociedade da FGV DIREITO RIO, respectivamente)

² <http://www.internetlab.org.br/pt/internetlab-reporta/internetlab-reporta-consultas-publicas-no-04/>

Se por um lado a redação atual do anteprojeto adota no artigo 5º inciso I uma definição abrangente de dados pessoais – que inclui dados relacionados à pessoa identificada ou identificável -, por outro, no inciso IV do mesmo artigo, dados anônimos são definidos de forma separada como aqueles em que não é possível se identificar o titular utilizando-se de meios razoáveis. Uma vez que no artigo 1º afirma-se que a lei dispõe sobre o tratamento de dados pessoais, parece haver uma exceção geral quanto aos dados anonimizados. Ainda que possam haver diversas interpretações sobre esse ponto, **o aparente conflito pode gerar insegurança jurídica no que diz respeito ao escopo de uma futura Lei de Proteção de Dados Pessoais,** principalmente se consideramos que a prática de anonimização de dados após certo período é corrente no mercado.

Além disso, esse tipo de exceção pode dar margem a uma relativização da proteção conferida à privacidade, especialmente nos casos em que práticas de desanonimização são utilizadas para se identificar o titular. É importante destacar que especialistas têm apontado para a fragilidade do conceito de anonimização de dados. **Para Cory Doctorow, “Quando uma regulamentação afirma que algum dado é “anônimo”, ela está desconectada das melhores teorias da ciência computacional”** (para mais informações, veja).

Uma boa prática seria estabelecer critérios claros para determinar o que seriam dados realmente anônimos e garantir que uma autoridade responsável pela implementação da lei – um órgão competente, como previsto no texto atual do anteprojeto – possa revisar esses critérios com base nos desenvolvimentos tecnológicos futuros. **Outra alternativa seria a de tornar efetivamente responsável aquele que adotar práticas falhas de anonimização pelos danos causados a um indivíduo que venha a ter seus dados pessoais eventualmente expostos.** Se por um lado, isso traria um incentivo a que certas informações sejam efetivamente deletadas ou desassociadas de um banco de dados anonimizado, por outro poderia desestimular práticas de big data. Com a evolução da tecnologia, existirá realmente banco de dados que não seja desanonimizável? E se não existir, faz realmente sentido excluir esses dados da proteção da lei? Dentro do que diz o anteprojeto, a diferença entre dados anônimos e dados pessoais está realmente apenas na possibilidade ou não de reidentificação?

Comentário: Jamila Venturini e Luiz Fernando Moncau (pesquisadora e gestor do Centro de Tecnologia e Sociedade da FGV DIREITO RIO, respectivamente)

Uma primeira interpretação sugere que um dado pessoal seria aquele capaz de levar diretamente a uma pessoa identificável (como um CEP, um endereço de IP, um identificador único de celular, etc.), enquanto o dado anônimo não poderia ser identificável nem com uso de “meios suscetíveis de serem razoavelmente utilizados para identificar o referido titular”. No entanto, nota-se que a definição atual de dados anônimos parece sugerir que sempre poderão haver meios – não razoáveis – para a reidentificação. Se é esse o caso, a diferença entre dados pessoais e anônimos residiria finalmente na conceituação de quais seriam meios razoáveis: se a reidentificação pode ser feita utilizando-se um meio razoável, estaríamos falando de um dado pessoal, caso contrário, o dado seria anônimo.

Nesse caso, parece adequado que o legislador forneça mais critérios para que se possa interpretar o que são meios razoáveis pra identificar o titular de um dado. O problema dessa alternativa é a de iniciar uma disputa interminável no campo legislativo, com barganhas acentuadas sobre os critérios de interpretação. Tal como na Europa, o lobby pelos interesses privados já avança no sentido de afirmar os benefícios do Big Data e a necessidade de excluir os dados anônimos de qualquer proteção. Os benefícios de qualquer atividade são inquestionáveis, mas a proteção dos direitos em um contexto de crescente potencial da tecnologia para invasão da privacidade merece especial atenção. E esse é o objetivo da lei. Tal como na Europa, este deve ser um ponto a levantar muita polêmica no decorrer do processo legislativo. Mais informações sobre técnicas de anonimização e seu debate na Europa podem ser encontradas aqui.

Por Dennys Antonialli, Jonas Coelho Marchezan, Francisco Brito Cruz e Mariana Giorgetti Valente

Sendo assim, propomos que seja alterada a redação do inc. I, do art. 5º:

I - dado pessoal: dado relacionado à pessoa natural identificada ou identificável, inclusive a partir de números identificativos, dados locais ou identificadores eletrônicos, **incluindo informações, isoladas ou agregadas, que possam sujeitar um indivíduo a um tratamento total ou parcialmente automatizado.**

Propomos, ainda, a seguinte redação para os inc. IV, V e VI, do art. 5º:

IV – anonimização: ato de tornar um dado não correlacionável ao seu titular, utilizando-se de técnicas que procurem não identificá-lo, direta ou indiretamente, com um indivíduo.

V – dados anônimos: dados relativos a um titular que não possa ser identificado, nem pelo responsável pelo tratamento nem por qualquer outra pessoa, tendo em conta o conjunto de meios suscetíveis de serem razoavelmente utilizados para identificar o referido titular;

VI – dados reidentificados: são dados pessoais em razão da possível reversibilidade do processo de anonimização.

Pelos mesmos fundamentos, propomos a exclusão do inc. XIV, do art. 5º.

IV – Consentimento

Consentimento e informação

A PROTESTE apoia a importância e o peso atribuído pela proposta de lei ao consentimento, nos termos do art. 7º, inclusive com destaque para o teor do § 1º, determinando que ele não pode condicionar o fornecimento de produto ou prestação de serviço; o § 5º, no sentido de que ele deve se referir à finalidades determinadas, considerando nulos os consentimentos genéricos; e o § 6º, habilitando o consumidor para revogar o consentimento a qualquer momento.

Entretanto, temos dúvida quanto à efetividade das disposições constantes do art. 10 para garantir que de fato a informação será dada ao cidadão de forma satisfatória, de modo a habilitá-lo a se decidir ou não pelo consentimento.

Isto porque, como é público e notório, são raros os casos em que as pessoas de fato leem os termos de uso, redigidos em geral de forma muito técnica, sem destaques e muito longos, o que desincentiva o usuário a se informar extensamente.

Sendo assim, propomos que se inclua no art. 10 referências no sentido de que os termos de uso devem ser redigidos de forma clara e simplificada.

Aderimos nesta parte à contribuição do GPOPAI da USP já na plataforma eletrônica de contribuições do APL de Proteção de Dados Pessoais, com o seguinte teor:

Há pelo menos três exemplos que podem ilustrar este argumento sobre simplificação e consolidação da mídia de comunicação com o usuário, são eles: (i) AVG PrivacyFix; (ii) Terms of Service; Didn't Read; e (iii) Lightbeam. Cada uma destas ferramentas oferece uma forma mais adequada de oferta e visualização de informações relevantes ao tratamento de dados do que documentos como termos e condições de uso e políticas de privacidade.

(...)

Acreditamos que o texto do Anteprojeto deve ser mais explícito sobre a necessidade da adoção de novas formas de apresentação de informações sobre o tratamento de dados.

(...)

Desta forma, não afirmamos que documentos como termos de uso ou políticas de privacidade são dispensáveis, contudo, não acreditamos que o modelo de consentimento deve ter estes documentos como principal canal de oferta e visualização de informações sobre o tratamento de dados.

Acreditamos que referidos instrumentos criam relações jurídicas importantes e devem ser preservados. É a sua leitura que não deve ser considerada como pressuposto do sistema, ou seja, não deve ser encarada como algo que o usuário irá se embasar para consentir o uso de suas informações. Assim, enfatizamos a necessidade de encontrar soluções mais eficientes para a forma de realização do consentimento do usuário, viabilizando a proposta para prestadores de serviço e usuários de forma menos onerosa.

Consentimento e dados reidentificados

Considerando nossa contribuição no sentido de tratar os dados reidentificados como dados pessoais, propomos a inclusão no art. 11, a fim de garantir que caso se reverta o processo de anonimização, para a utilização dos dados será necessário obter o consentimento expresso do titular.

O caput do art. 11

Propomos a seguinte redação para o *caput* do art. 11:

Art. 11. O consentimento será dispensado quando os dados forem de acesso público irrestrito E quando o tratamento for indispensável para:

De acordo com a proposta de lei, o tratamento dos dados deve obedecer os princípios da finalidade, adequação e necessidade. Desta forma, não basta que os dados sejam de acesso público, mas também que seja indispensável a sua utilização, nos termos dos incs. I, II e III, do art. 6º.

O inc. II, do art. 11

Propomos a seguinte redação para o inc. II, do art. 11:

II – tratamento e uso compartilhado de dados relativos ao exercício de direitos ou deveres previstos em leis ou regulamentos pela administração pública, ***garantida, sempre que possível, a anonimização dos dados pessoais;***

Tendo em vista as garantias constitucionais de respeito à privacidade e intimidade, a lei de proteção de dados pessoais deverá impor à administração pública a regra da anonimização, a fim de minimizar o grau de vulnerabilidade dos cidadãos frente aos poderes estatais.

O inc. III, do art. 11

Propomos a seguinte redação para o inc. III, do art. 11:

III – execução de obrigações relacionadas a um contrato do qual é parte o titular, observado o disposto no § 1º, do art. 6º, ***garantida, sempre que possível, a anonimização dos dados pessoais;***

Entendemos que não há nenhuma justificativa para que o consentimento seja dispensado na fase pré-contratual. É importante que o cidadão ou consumidor estejam cientes de que nesta fase seus dados serão analisados, a fim de que autorize ou não o tratamento e possa, também, decidir se quer ou não dar continuidade ao processo de contratação. Por outro lado, não há prejuízos para o fornecedor ou poder público em obter o consentimento. A

regra deve ser: sempre que houver a coleta e tratamento de dados, deve haver o correspondente consentimento.

V – Dos dados pessoais sensíveis

A PROTESTE manifesta seu apoio incondicional ao art. 12, entendendo que traz dispositivos fundamentais para reduzir significativamente os riscos de utilização discriminatória dos dados sensíveis.

A fim de reforçar a proteção de dados sensíveis e dar maior importância ao consentimento como instrumento de controle dos dados pelo titular, propomos a seguinte redação para o § 1º, do art. 13:

§ 1º A realização de determinadas modalidades de tratamento de dados pessoais sensíveis poderá ser condicionada à autorização prévia de órgão competente, ***bem como de consentimento especial do titular***, nos termos do regulamento.

Vale aqui destacar que a lei não especifica a quem caberá editar o regulamento, o que termina por fragilizar a efetividade do dispositivo, na medida em que, até que se constitua um órgão competente, este direito não se materializa.

VI – Término do tratamento

Propomos a seguinte redação ao inc. II, do art. 15:

II – pesquisa histórica, científica ou estatística ***vinculada à política pública***, garantida, sempre que possível, ***a anonimização*** dos dados pessoais; ou

Nossa proposta se baseia na garantia de que empresas não se utilizarão dos dados para estatísticas de interesse privado.

A dissociação é uma espécie do gênero anonimização, razão pela qual entendemos que haverá mais garantia se a lei utilizar termo mais abrangente.

Propomos a seguinte redação ao inc. III, do art. 15:

III – ***no caso de cessão dos dados a terceiros, o responsável deverá cumprir o disposto no § 5º, do art. 17.***

VII – Direitos do Titular

Propomos a seguinte redação ao inc. IV, do art. 17:

IV – ***anonimização***, bloqueio ou cancelamento de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta lei.

Substituímos o termo dissociação por anonimização pelas razões já expostas acima.

Propomos a inclusão dos seguintes incisos ao art. 17:

V – exclusão do banco de dados por interesse do titular;

VI – portabilidade por interesse do titular ou, sendo por interesse do responsável, ao consentimento prévio.

Considerando as premissas sobre as quais se desenvolveu o texto da proposta de lei, entendemos que o consumidor ou cidadão tem sempre a condição de titular de seus dados e, portanto, deve ter o direito de requerer a exclusão quando for cabível.

Invocamos a mesma justificativa para a introdução do direito à portabilidade.

VIII – Comunicação e Interconexão

Sobre o mesmo fundamento a respeito da titularidade dos dados pessoais, propomos que sejam retirados do art. 24 todos os incisos e parágrafo único, que estabelecem exceções ao direito do titular dos dados de consentir livre, expressa e especificamente, quando se tratar de comunicação ou interconexão entre pessoa de direito público e pessoa de direito privado.

Sendo assim, propomos a seguinte redação ao art. 24:

Art. 24. A comunicação ou interconexão de dados pessoais entre pessoa jurídica de direito público e pessoa de direito privado dependerá de consentimento livre, expresso, específico e informado do titular.

Propomos a adequação do tempo verbal do vocábulo realizar utilizado no art. 26, nos seguintes termos:

Art. 26. O órgão competente poderá solicitar, a qualquer momento, aos órgãos e entidades públicos que ***realizam*** interconexão de dados e o uso compartilhado de dados pessoais, informe específico sobre o âmbito, natureza dos dados e demais detalhes do tratamento realizado, podendo emitir recomendações complementares para garantir o cumprimento desta Lei.

IX – Transferência internacional de dados

Propomos a retirada do art. 29, na medida em que a transferência de dados para países que não apresentem em seus ordenamentos jurídicos instrumentos de proteção dos dados pessoais, termina por colocar o cidadão ou consumidor em situação de extrema vulnerabilidade.

As previsões dos incs. I e II, para que o titular seja previamente informado quanto aos riscos, a fim de manifestar seu consentimento, não é suficiente. Trata-se de situação com alto grau de complexidade a respeito da qual o titular tem condições muito reduzidas de formar um juízo a respeito.

X – Responsabilidade dos Agentes

Propomos alterar a redação do § 2º, do art. 35, nos seguintes termos:

§ 2º A responsabilidade é objetiva e solidária respondendo o responsável e o operador, ressalvado o direito de regresso em processo ou procedimento posterior quando será apurada a culpa.

Entendemos que não há justificativa para que a responsabilização decorrente de ato ilícito praticado por qualquer dos agentes que atuem na cadeia de coleta e tratamento de dados seja subjetiva, dependendo da apuração de culpa, o que prolongará o curso de processo judicial, prejudicando injustamente o cidadão ou consumidor.

Defendemos que a responsabilidade deve seguir o mesmo regime estabelecido pelo Código de Defesa do Consumidor.

Propomos a seguinte redação para o art. 38:

Art. 38. As competências e responsabilidades relativas à gestão de bases de dados nos órgãos e entidades públicos, bem como a responsabilidade pela prática de atos administrativos referentes a dados pessoais, ***serão objetivas, ressalvado o direito de regresso por dolo ou culpa, nos termos do art. 37, § 6º, da Constituição Federal.***

Entendemos que a lei não pode restringir um direito estabelecido expressamente pela Constituição Federal.

XI – Responsável e Operador

Propomos a seguinte redação para o parágrafo único do art. 40:

Parágrafo único. Órgão competente ***deverá*** dispor sobre formato, estrutura e tempo de guarda do registro.

Trocamos o verbo poderá por deverá, na medida em que os temas sobre os quais o dispositivo trata são de grande relevância para que o cidadão ou consumidor possam exercer o direito de controle sobre seus dados e, portanto, entendemos que a definição das regras não podem ficar no campo da discricionariedade, devendo ser definidas o mais rápido possível.

XII – Sanções administrativas

Propomos a seguinte redação ao inc. III, do art. 50:

III – a ***anonimização*** dos dados pessoais;

Invocamos a justificativa já mencionada anteriormente para a troca do termo dissociação por anonimização.

Propomos a inclusão do seguinte parágrafo §º ao art. 50:

§ 3º - aos órgãos e entidades públicos só serão impostas as sanções estabelecidas pelos incs. II e III do art. 50, devendo o órgão competente estabelecer prazo para a adequação das condutas aos termos da lei, sem prejuízo da responsabilidade pessoal dos agentes.

Entendemos que as sanções estabelecidas nos demais incisos, se aplicadas aos órgãos públicos, implicarão em prejuízo injustificado para a administração pública, bem como no comprometimento de atribuições que lhes são peculiares, em prejuízo dos administrados e de políticas públicas.

Esperando estar contribuindo para o processo de edição de importante ferramenta legal para a garantia da privacidade e dados pessoais, tratando de atividades comerciais e públicas que impactam fortemente este direito já reconhecido pela Declaração Universal dos Direitos Humanos das Nações Unidas, a PROTESTE saúda o Ministério da Justiça por adotar processo democrático, abrindo canais de participação à sociedade brasileira.

Flávia Lefèvre Guimarães

Conselho Consultivo da PROTESTE