À COMISSÃO ESPECIAL DE TRATAMENTO E PROTEÇÃO DE DADOS PESSOAIS DA CÂMARA DOS DEPUTADOS

Referência: Audiência pública sobre Comissão Especial destinada a proferir Parecer ao Projeto de Lei nº 4060, de 2012, do Dep. Milton Monti, que "dispõe sobre o tratamento de dados pessoais, e dá outras providências".

O **Instituto Brasileiro de Defesa do Consumidor** (Idec) vem perante a ilustre Comissão Especial de Tratamento e Proteção de Dados Pessoais da Câmara dos Deputados apresentar, em audiência pública, seu posicionamento sobre os Projetos de Lei 5.276/16 e 4.060/12, que tramitam em conjunto perante esta casa legislativa.

O Idec é uma instituição sem fins lucrativos que desde 1987 realiza atividades em prol do consumidor brasileiro, que vão de testes de produtos a ações judiciais coletivas, com enfoque na defesa dos direitos coletivos. O Idec atuou na formulação do Código de Defesa dos Consumidores (1990) e nas campanhas em defesa do Marco Civil da Internet (2014).

O Idec é membro pleno da *Consumers International* e faz parte do Fórum Nacional das Entidades Civis de Defesa do Consumidor e Associação Brasileira de Organizações Não-Governamentais. Em 2016, o Instituto tornou-se membro do *Civil Society Information Society Advisory Council* (CSISAC), que representa a sociedade civil perante o Comitê de Políticas para Economia Digital da Organização para Cooperação e Desenvolvimento Econômico (OCDE). O Idec também colaborou com a Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD) na elaboração de uma pesquisa comparativa sobre níveis de proteção de dados pessoais.[1]

O presente documento pretende sintetizar o posicionamento do Idec no que toca ao

[1] UNCTAD. *Data Protection Regulations and International Data Flows: implications for trade and developments*. United Nations, 2016. Disponível em: http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf

nível de proteção de dados pessoais desejável no Brasil. Em especial, nos preocupamos em refutar algumas das teses apresentadas no documento *Manifesto Sobre a Futura Lei de Proteção de Dados Pessoais*, publicado em setembro de 2016 por uma ampla coalizão de empresas do setor de tecnologia e publicidade.[2]

O referido manifesto apresenta graves distorções aos principais conceitos dos projetos de lei em discussão no Congresso Nacional, em especial o conceito de *dado pessoal*, o conceito de *dados sensíveis* e as regras de *responsabilização civil*. Como será explicitado nas próximas páginas, a posição do manifesto precisa ser refutada em detalhes, sob o risco de gerar graves prejuízos aos consumidores nas relações de consumo do século XXI – todas elas potencialmente mediadas por dispositivos sensores, microprocessadores de dados e capacidade de comunicação com outras bases via Internet.

O uso de dados pessoais estará presente massivamente no cotidiano dos consumidores. É preciso cautela para definição dos conceitos legais e do modelo regulatório para proteção dos dados pessoais criado no Brasil, com aderência aos princípios do Código de Defesa do Consumidor.

1. O resgate ao conceito de "dado pessoal"

Uma lei de proteção de dados pessoais tem como sua espinha dorsal o conceito de *dado pessoal*. O manifesto apresentado pelas empresas a esta Comissão defende que "um conceito amplo de dado pessoal pode inibir o desenvolvimento da economia e inovação baseada em dados" e que "uma conceituação ampla tornaria praticamente todos os dados produzidos pela atividade humana sujeitos à lei". Assim, propõem que dado pessoal seja definido como "qualquer dado que identifique de forma exata e precisa uma pessoa natural".

Essa definição *altamente restritiva* não encontra paralelo tampouco na legislação brasileira. Em 2011, a Lei de Acesso à Informação (LAI) definiu que dados pessoais (ou *informações pessoais*, na terminologia daquela lei) são aqueles "aquela relacionada à pessoa

[2] O manifesto foi elaborado por Brasscom, Camara-e.net, Assespro, Associação Nacional de Bureaus de Crédito (ANBC), Abranet, ABES Software, e está disponível em: http://www.brasscom.org.br/brasscom/upload/posicionamento/1480521390doc-2016-050_(manifesto_protecao_de_dados_pessoais)_v37.pdf

natural identificada ou *identificável*" (Lei 12.527/11, art. 4º, IV). É crucial explicar por que inclui-se a palavra *relacionado à pessoa identificável* nas principais legislações ao redor do mundo.

Se considerarmos como dado pessoal apenas os dados relacionados à pessoa identificada, nos referimos às informações que as pessoas "sabem de cor" como o endereço, o telefone, o número do RG, o número do CPF. Nas economias digitais e das discussões sobre privacidade, isso é muito pouco. A verdadeira "mina de ouro", capaz de relevar quase tudo sobre uma pessoa, está nos dados relacionados a uma pessoa identificável, como os dados de geolocalização, as informações sobre o uso de dispositivos, os endereços *Internet Protocol* (IP) e as informações produzidas por uma pessoa por meio da fala ou pela utilização de tecnologias. É a combinação desses dados aparentemente neutros que gera a criação de perfis individuais, dando origem a um lucrativo mercado com finalidades diversas (identificação individual, controle de fraudes ou publicidade comportamental). Em 2012, no relatório *Protecting Consumer Privacy in an Era of Rapid Change* elaborado pela Federal Trade Commission, reconheceu-se que "há suficientes evidências demonstrando que os avanços tecnológicos e a habilidade de combinar diferentes conjuntos de dados pode levar à identificação de um consumidor, um computador ou um dispositivo, mesmo que as partes individuais desse conjunto não constituam *personally identifiable information*"[3].

Essa definição consolidou-se na Diretiva nº 95/46/CE, aprovada pelo Parlamento Europeu em 24 de outubro de 1995, que determinou que os dados pessoais são relacionados à pessoa "identificada" e também "identificável". Em 2016, o Regulamento 2016/679 do Parlamento Europeu, de 27 de abril de 2016, que revogou a influente Diretiva 95/46/CE deliberou que:

> "Os princípios da proteção de dados pessoais deverão aplicar-se a qualquer informação relativa a uma pessoa singular identificada ou identificável. Os dados que tenham sido pseudonimizados, que possam ser atribuídos a uma pessoa singular mediante a utilização de informações suplementares, deverão

[3] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change. Report. Washington: FTC, 2012, p. 20. Disponível em: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

> ser considerados informações sobre uma pessoa identificável. Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular" (26).

Na legislação europeia, que serve de referência para a construção dos modelos regulatórios na América Latina, determina-se também que as pessoas singulares "podem ser associadas por via eletrônica, fornecidos pelos respectivos aparelhos, aplicações, ferramentas e protocolos, tais como endereços IPS ou testemunhos de conexão (cookies) ou outros identificadores, como as etiquetas de identificação por radiofrequência". Como ressaltado na nova legislação do Parlamento Europeu, "*estes indicadores podem deixar vestígios que, em especial quando combinados com identificados únicos e outras informações recebidas pelos servidores, podem ser utilizados para a definição de perfis e a identificação de pessoas singulares*"[4]. De acordo com o novo regulamento de proteção de dados pessoais na Europa (art. 4º):

> "Entende-se por dados pessoais, informação relativa a uma pessoa singular identificada ou identificável (titular dos dados); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de geolocalização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular"[5].

É acertada a definição do Projeto de Lei nº 5.276/16, fruto de debates com organizações de defesa dos consumidores, entidades de pesquisa, acadêmicos e empresários. No art. 5º, inciso I, dispõe-se que dado pessoal é o *dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa*.

Tal definição também encontra respaldo legal no decreto de regulamentação do Marco

[4] Regulamento 2016/679 do Parlamento Europeu, Considerando nº 30.
[5] Regulamento 2016/679 do Parlamento Europeu, Artigo 4º ("Definições").

Civil da Internet (Lei 12.965/14), que consagra a proteção de dados pessoais como um dos pilares principiológicos do uso da Internet no Brasil. No capítulo III do decreto, que trata "da proteção aos registros, aos dados pessoais e às comunicações privadas", determina-se, no art. 14, que dado pessoal é "dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa"[6].

Essa definição está completamente alinhada com países que se preocupam com a proteção de direitos fundamentais e exigem proporcionalidade na definição de regras de mercado, como é o caso do regime jurídico brasileiro, moldado pelas regras gerais da Constituição Federal e do Código de Defesa do Consumidor. A concepção *ampliada* de "dados pessoais" também encontra respaldo na crescente literatura sobre o direito à proteção dos dados pessoais no Brasil.[7]

Como evidencia o relatório de análise do processo de consulta pública do anteprojeto de lei de proteção de dados pessoais de 2015, elaborado pelo InternetLab, nenhuma entidade de defesa dos consumidores e nenhum centro de pesquisa independente defendeu uma concepção restritiva de dados pessoais. Os que defenderam concepções restritivas na consulta de 2015 foram Câmara BR, Boa Visto Serviços, Cisco, BSA, MPA, ITI, US Business Council, IAB, Abranet, Febraban e outros.[8]

Uma definição *restritiva* de dados pessoais só atende aos interesses de empresas, de diferentes setores, interessadas na livre exploração do novo "mercado dos dados", em um ambiente completamente desregulamentado, deixando os cidadãos desprotegidos e sem amparo legal.

---

[6] Decreto 8.771, de 11 de maio de 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm

[7] CASTRO, Luiz Fernando Martins. Proteção de dados pessoais-panorama internacional e brasileiro. Revista CEJ, v. 6, n. 19, p. 40-45, 2002. DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. GEDIEL, José Antônio Peres; CORRÊA, Adriana Espíndola. Proteção jurídica de dados pessoais: a intimidade sitiada entre o Estado e o mercado. Revista da Faculdade de Direito UFPR, v. 47, 2008. LOUZADA, Luiza; VENTURINI, Jamila. A regulamentação de proteção de dados pessoais no Brasil e na Europa: uma análise comparativa. Fundação Getulio Vargas, 2015.

[8] InternetLab, *O Que Está em Jogo no Debate sobre Dados Pessoais no Brasil?*. São Paulo: InternetLab, 2015, p. 49-50. Disponível em: http://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf

Essa visão restritiva deve ser rejeita pela Comissão, pois criaria um retrocesso jurídico que é contrário à legislação nacional (Lei de Acesso à Informação e decreto de regulamentação do Marco Civil da Internet), o posicionamento da doutrina jurídica e o conceito discutido em profundidade, durante mais de cinco anos, no período de formulação do anteprojeto de lei de proteção de dados pessoais, conduzido pelo Ministério da Justiça.

2. Biometria, dados sensíveis e as regras do jogo

Entendemos que a Comissão deve prestar especial atenção ao conceito de dados sensíveis e dados que, pela sua natureza, são sensíveis do ponto de vista de direitos e liberdades fundamentais.

Existem diferenças sutis entre a proposta das empresas (manifesto), o conceito proposto no projeto de lei 5.276/16 e a definição mais atual aprovada no Parlamento Europeu. O regulamento europeu não utiliza o conceito de "dados sensíveis" no capítulo de definições, mas cria uma regra de "tratamento de categorias especiais de dados especiais". Vejamos tais diferenças:

Tabela 1. Definições de dados sensíveis ou limitações (Manifesto, PL 5276 e Parlamento Europeu)

Origem	**Texto legal**
Manifesto empresarial (setembro de 2016)	"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 à condição médica do titular, genéticos e referentes à orientação afetiva e de gênero"
PL 5.276 (maio de 2016)	"Dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos"
Regulamento Europeu (abril de 2016)	"É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa"

Fonte: elaboração própria a partir de documentos disponíveis online

Note-se que o manifesto defendido pelas empresas no Brasil tenta *excluir os dados biométricos* do âmbito de proteção dos dados sensíveis. Tal estratégia tem sido defendida, há anos, pela Febraban para que os dados biométricos sejam livremente utilizados no setor financeiro e, com a popularização das tecnologias de biometria, no setor de comércio eletrônico e de pagamentos.

Os dados biométricos são dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que *permitam ou confirmam a identificação única dessa pessoa singular*. Trata-se de um dado altamente sensível, pois ele é inequívoco e pode ser combinado com técnicas de identificação capazes de identificar individualmente uma pessoa em qualquer parte do mundo. Um registro gerado a partir de sua íris gera uma identificação única e inequívoca de uma pessoa. Não há possibilidade de registros duplos, o que faz com que esse dado seja um tipo especial de dado pessoal, que necessita de mais cautela.

Técnicas avançadas de fotografias e reconhecimento facial também podem ser gerar dados biométricos. No regulamento europeu, determina-se que o tratamento de fotografias pode implicar nas regras e limitações de tratamento de dados biométricos quando "forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular".

Resgatamos aqui o que foi sinalizado pelo InternetLab em seu relatório de 2015 sobre a consulta do anteprojeto de lei de proteção de dados pessoais e a proposta de abrangência dos dados sensíveis para inclusão dos dados biométricos, defendido por entidades de defesa do consumidor, pela Fiesp e pelo GPOPAI/USP:

> "Os dados biométricos seriam identificadores únicos em razão do seu grau de precisão. Dada a característica imutável do corpo de uma pessoa, eles seriam mais singulares até que outros tipos de dados pessoais usados para a identificação de uma pessoa. Por exemplo, os registros de identidade e o número no cadastro nacional de pessoas físicas. Por tal razão, eles deteriam um potencial lesivo elevado, pois, a partir deles, seu titular extaria exposto aos

mais variados tipos de fraudes e roubos de identidade" [9].

Entendemos que é papel da Comissão defender a manutenção dos dados biométricos como dados sensíveis, passíveis de maior tutela jurídica. Além de ser coerente com os desenvolvimentos jurídicos mais relevantes em perspectiva internacional, essa proposta aprofunda os princípios de proteção da vida e segurança dos consumidores, tal como definido no Código de Defesa do Consumidor. Considerando que o potencial lesivo é maior, o tratamento de dados sensíveis (incluindo dados biométricos) só pode ocorrer se houver consentimento explícito para o tratamento desses dados para *finalidades específicas*, seguindo a arquitetura de princípios proposta no art. 6º do projeto de lei 5.276/16.[10]

Nesse sentido, a proposta de determinadas empresas de que o tratamento de dados sensíveis "prescinda de consentimento diferenciado" em razão de "disponibilização voluntária" e "manifestação da liberdade de expressão" é flagrantemente inadequada em termos jurídicos. Os dados sensíveis necessitam de tratamento especial com consentimento explícito e finalidade legítima, sendo inadequado criar uma regra de livre coleta sob o pretexto de defesa da liberdade de expressão.

3. A responsabilização civil e a defesa dos princípios consumeristas

O último ponto que gostaríamos de tratar neste texto é a tentativa de inversão da regra de responsabilidade solidária na cadeia de fornecedores de serviços, um dos princípios consagrados do Código de Defesa do Consumidor e reconhecido, de forma pacífica, pelo Superior Tribunal de Justiça.

O manifesto empresarial direcionado à Comissão afirma que, "no descumprimento de

[9] InternetLab, *O Que Está em Jogo no Debate sobre Dados Pessoais no Brasil?*. São Paulo: InternetLab, 2015, p. 56. Disponível em: http://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf

[10] Os princípios são finalidade (as finalidades devem ser legítimas, específicas, explícitas e informadas ao titular), adequação (compatível com as finalidades e legítimas expectativas do titular), necessidade (o tratamento deve se limitar ao mínimo necessário para a realização das finalidades), livre acesso (titulares podem consultar as modalidades de tratamento facilmente), qualidade (exatidão, clareza e atualização dos dados), transparência (informações claras e acessíveis sobre agentes que tratam os dados), segurança (medidas técnicas e administrativas para proteger os dados de acesos não autorizados e situações acidentais), prevenção (prevenir ocorrência de danos), não discriminação (tratamento não pode ser feito para fins discriminatórios).

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".

O argumento apresentado é que, por serem pessoas jurídicas diversas e independentes, as empresas não podem "exercer controle sobre as atividades umas das outras". Assim, não seria "razoável atribuir-se responsabilidade solidária entre elas por atos sobre os quais não podem ter poder de supervisão que lhes permita controlar e evitar os prejuízos que serão obrigadas a reparar".

Trata-se de argumento falho, que não se sustenta no direito brasileiro. O Código de Defesa do Consumidor tem, em seu artigo 14, uma regra geral sobre o assunto. Diz que "o fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços". Por serviço defeituoso, entende-se quando não fornece a segurança que dele pode esperar, como é o caso de segurança no tratamento de dados pessoais coletados para oferecimento de determinados serviços.

Felizmente, o projeto de lei 5.276/16 prevê um conjunto de regras sobre responsabilidade e ressarcimento de dados, seguindo a lógica do art. 14 do Código de Defesa do Consumidor:

> "Art. 42. **Todo aquele que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, é obrigado a repará-lo**.
> Parágrafo único. O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
> Art. 43. A eventual dispensa da exigência do consentimento não desobriga os agentes do tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.
> Art. 44. Nos casos que envolvem a transferência de dados pessoais, o cessionário ficará sujeito às mesmas obrigações legais e regulamentares do cedente, **com quem terá responsabilidade solidária pelos danos**

> **eventualmente causados**.
> Parágrafo único. A responsabilidade solidária não se aplica aos casos de tratamento realizado no exercício dos deveres de que trata a Lei nº 12.527, de 2011, relativos à garantia do acesso a informações públicas".

É justamente essa regra que as empresas querem confrontar. Eliminar a regra de responsabilidade solidária do projeto de lei de proteção de dados pessoais, no entanto, **pode gerar consequências danosas aos consumidores**, além de ser contrário ao art. 14 do Código de Defesa do Consumidor.

O consumidor, por ser a parte hipossuficiente na relação de consumo, não possui condições de mapear toda a rede de empresas subcontratadas por uma empresa que coleta seus dados pessoais. É absolutamente desleal exigir que os consumidores acionem empresas subcontratadas que podem estar em qualquer lugar do mundo. As empresas que possuem o dever de diligência na seleção de parceiros comerciais. O consumidor está apenas em uma das pontas de um emaranhado de relações jurídicas, sendo que a responsabilidade solidária existe para proteger os direitos dos consumidores.

O microssistema jurídico criado pelo Código de Defesa do Consumidor tem sido reconhecido por diversas decisões do Superior Tribunal de Justiça envolvendo prestadores de serviços e utilização de bancos de dados. Em uma decisão paradigmática de 2014 – o Recurso Especial 1419697/RS, Segunda Seção, Relator Ministro Paulo de Tarso Sanseverino –, o STJ firmou o seguinte entendimento:

> "O desrespeito aos limites legais na utilização do sistema "credit scoring", configurando abuso no exercício desse direito (art. 187 do CC), **pode ensejar a responsabilidade objetiva e solidária do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consulente (art. 16 da Lei n. 12.414/2011) pela ocorrência de danos morais nas hipóteses de utilização de informações excessivas ou sensíveis** (art. 3º, § 3º, I e II, da Lei n. 12.414/2011), bem como nos casos de comprovada recusa indevida de crédito pelo uso de dados incorretos ou desatualizados".

Além da dimensão principiológica do CDC, é importante lembrar que o Marco Civil

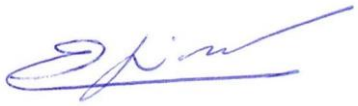
da Internet (Lei 12.965/14) também prevê situações de responsabilidade solidária em casos de empresas estrangeiras envolvidas em determinada cadeia de fornecimento de serviços e ofensa aos 10 e 11, que tratam da coleta de dados pessoais por provedoras de aplicações:

> "Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
> § 1º O disposto no **caput** aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
> § 2º O disposto no **caput** aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.
> § 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.
> § 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.
> Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;
> III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou
> IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.
> Parágrafo único. **Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o caput sua filial, sucursal, escritório ou estabelecimento situado no País**".

A defesa do consumidor é um dos pilares do Marco Civil da Internet (art. 2º, Lei

12.965/14), do mesmo modo que é um dos pilares da proteção dos dados pessoais, conforme art. 2º do projeto de lei 5.276/16. Só é possível ter coerência com a defesa dos consumidores **mantendo a regra basilar de responsabilidade solidária**, refutando a proposta do manifesto empresarial aqui analisado.

Esperamos, com esses breves comentários sobre três pontos específicos – o conceito de dado pessoal, as regras para tratamento de dados sensíveis e as regras de responsabilidade solidária –, ter contribuído para a análise do projeto de lei de proteção de dados pessoais sob a perspectiva da defesa do consumidor. Ficamos à disposição desta Comissão Especial para a análise de outros pontos prioritários que não foram tratados neste texto e que merecem escrutínio público.



Elici Mª Checchin Bueno
Coordenadora Executiva
Instituto Brasileiro de Defesa do Consumidor

Rafael A. F. Zanatta
Pesquisador em Telecomunicações – Idec