

Ilustríssima Senhora Presidente da Comissão Especial de Tratamento e Proteção de Dados Pessoais (PL 4060/2012 | PL 5276/2016) da Câmara dos Deputados, Deputada Federal Bruna Furlan

A/C

Secretaria-Executiva da CESP Dados Pessoais

ce.dadospessoais@camara.leg.br

1. A **ABRANET – Associação Brasileira de Internet**, fundada em 1996, com o objetivo de congregar os provedores de Internet e atuar em defesa da Internet, saudando a iniciativa desta Comissão Especial de promover o debate público sobre o tema do Tratamento e Proteção de Dados Pessoais, apresenta suas contribuições ao debate legislativo.

Introdução

2. Esta manifestação está estruturada, além desta breve introdução, em duas seções. Na Seção I são apresentadas algumas linhas sobre a importância da proteção de dados para a economia e sociedade digital, e na Seção II estão os comentários da ABRANET sobre os principais temas que permeiam o debate legislativo, não apenas no Brasil, mas também em outras jurisdições, tais como: (i) conceitos de “*dado pessoal*”, “*dados anônimos*”; (ii) forma de consentimento; (iii) reconhecimento do “legítimo interesse” (iv) aplicação ao Estado e proteção dos direitos fundamentais do titular; (v) segredo industrial; (vi) transferência internacional de dados; (vii) autoridade competente; (viii) *vacatio legis*.
3. Ao final, a ABRANET apresenta um quadro anexo, no qual suas principais sugestões e comentários à atual redação do PL 5276/16 encontram-se consolidados de forma mais sistemática.

Seção I. A importância da adequada proteção de dados para o equilíbrio entre economia e sociedade digital

4. A economia digital que vivemos, cuja marca é expansão da Internet sobretudo após os anos 90, trouxe um mundo mais conectado, inclusivo e cada vez mais inteligente. Dentro desse contexto da economia digital, o desafio é criarmos normas que, ao mesmo tempo em que assegurem as liberdades individuais, estimulem o empreendedorismo e tragam segurança jurídica para que as empresas possam investir e permitam a geração de novos empregos e riquezas para nosso país¹, ou seja, além de assegurar as liberdades individuais, também assegurem a liberdade de iniciativa, geradora de bem-estar social.
5. É neste contexto que os negócios baseados em dados crescem exponencialmente e, segundo dados da BRASSCOM² prevê-se ganhos de eficiência que podem agregar cerca de US\$ 15 trilhões ao PIB global até 2030, beneficiando vários setores, tais como, agricultura, transporte, saúde etc.
6. Vivemos hoje em uma nova “era digital” que é baseada e guiada por megadados (“*Big Data*”), pela Internet das Coisas (*Internet of Things – IoT*), Inteligência Artificial (*Artificial Intelligence – AI*) e pelo aprendizado de máquinas (*Machine Learning*). Dados fluem no mundo em volume constantemente crescente e são utilizados em maneiras novas e cada vez mais complexas. Isso constitui uma nova realidade que tem que ser levada em consideração quando da elaboração de novas leis de privacidade e proteção de dados que

¹ [...] a nova economia é a economia da indústria da internet. Em outra abordagem, observamos o crescimento de uma nova economia a partir de dentro da velha economia, como o resultado do uso da Internet pelas empresas, para o seu próprio objetivo e em contextos específicos, CASTELLS, Manuel. A galáxia da Internet: reflexões sobre a internet, os negócios e a sociedade. Tradução Maria Luiza X. de A. Borges; revisão técnica Paulo Vaz. Rio de Janeiro: Jorge Zahar, 2013, p. 10. Além disso, “Do redemoinho das empresas ponto.com resultou uma nova paisagem econômica, com as empresas eletrônicas em seu núcleo. Por empresas eletrônicas entendo qualquer atividade de negócio cujas operações-chave de administração, financiamento, inovação, produção, distribuição, vendas, relações com empregados e relações com clientes tenham lugar predominantemente pela/na Internet ou outras redes de 55 computadores, seja qual for o tipo de conexão entre as dimensões virtuais e físicas da firma”. (CASTELLS, Manuel. A galáxia da Internet: reflexões sobre a internet, os negócios e a sociedade. Tradução Maria Luiza X. de A. Borges; revisão técnica Paulo Vaz. Rio de Janeiro: Jorge Zahar, 2013).

² Pesquisa apresentada em consulta pública realizada em 07/07/2016 para a Comissão de Trabalho, de Administração e Serviço Público e Comissão de Ciência e Tecnologia, Comunicação e Informática, disponível no link <http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/cctci/Eventos/2016/07-07-2016-smc-pl-5276-2016-dados-pessoas-da-pessoa-natural/sergio-gallindo-brasscom>

se adequem a nova era de informações. O Brasil tem a oportunidade singular de criar uma lei que atenda às necessidades dessa era digital, levando em consideração as experiências, erros e acertos de outros regimes de privacidade pelo mundo. A maioria, quiçá todos, desses regimes de privacidade que existem historicamente foram projetados antes da era digital e também enfrentam hoje a necessidade de se modernizarem.

7. Esse cenário nos demonstram a relevância do tema tratado esta Ilustre Comissão Especial para o futuro da economia brasileira, cujo desenvolvimento é condição não apenas para a existência de um mercado próspero, mas também para a dignidade dos cidadãos brasileiros. Desta forma, na próxima seção, serão apresentados de forma consolidada os comentários da ABRANET sobre os principais temas elencados nesta Iniciativa Legislativa, mas que certamente não esgotam a disposição para contribuições técnicas e jurídicas de nossa associação para este tema de tanta relevância para o país

Seção II. Nossa Visão sobre o Projeto de Lei

8. A discussão sobre proteção de dados possui um desafio central: como o ordenamento jurídico deve lidar com os impactos das novas tecnologias de maneira construtiva, protegendo o cidadão e, ao mesmo tempo, impulsionando as atividades econômicas baseadas em dados? Em outros termos, como proteger as informações e o cidadão sem regular em demasia mercados ainda nascentes, o que acabaria por engessar ou condenar esses mercados e principalmente o desenvolvimento econômico nacional?
9. Na visão da ABRANET, um projeto de lei de proteção de dados pode perfeitamente superar esse desafio e impulsionar a economia digital, criando um arranjo institucional e normativo que favoreça a aplicação da forma motriz do ordenamento: os princípios constitucionais e específicos para a atividade. Os princípios, se de um lado são os instrumentos jurídicos mais potentes e que irradiam por todo ordenamento, de outro, são atemporais, ou seja, passíveis de convivência futura com os novos instrumentos e mercados de tecnologia. Nesse passo, o projeto de lei de proteção de dados em discussão nesta I. Comissão Especial merece ser louvado por incorporar em seu texto objetivos como privacidade, liberdade de expressão e iniciativa, dentre outros princípios.

10. Vale destacar que a ABRANET também reconhece os princípios relacionados à proteção e tratamento de dados universalmente aceitos, tais como finalidade, transparência, adequação, qualidade dos dados, segurança, prevenção, etc. Por isso, os comentários e sugestões apresentados não tratam, de nenhuma forma, de suprimi-los ou reduzi-los. O objetivo geral das sugestões é contextualizar os princípios dentro do ambiente contemporâneo em que o tratamento de dados pessoais em grande escala é inerente à sociedade, realidade essa que tende a se intensificar com a consolidação da “Internet das Coisas” e expansão do conceito do “Big Data”.
11. Por fim, a ABRANET entende que é de grande importância o reconhecimento de que a economia de dados é uma realidade mundial e que o Brasil deve posicionar-se como protagonista neste cenário.

II. 1 Conceitos de “dado pessoal” e “dados anônimos”

12. A ABRANET entende que o conceito de “dado pessoal” merece uma definição pragmática, calcada na probabilidade de o dado efetivamente levar à identificação de um indivíduo determinado, em outras palavras a definição de “dado pessoal” deve estar relacionada a uma pessoa identificada ou identificável no nível individual. Neste sentido, apresenta-se a seguinte sugestão de redação:

Dado pessoal: dado relacionado à pessoa natural identificada ou identificável no nível individual.

13. Já com relação ao termo “dado anônimo”, para que se vença o desafio regulatório supra mencionado, ou seja, ao mesmo tempo que seja tutelado o dado pessoal, proteja-se a florescência de economia de dados e, principalmente, sejam criados parâmetros de legitimidade para o trabalho das empresas sérias com dados que não levem à identificação de pessoas, é igualmente importante que seu conceito seja assertivo.
14. Do ponto de vista jurídico, se está diante de situação de graus distintos de proteção, necessários, ademais, para que se possa impulsionar um ambiente institucional que favoreça o respeito à proteção efetiva dos dados pessoais, separando, com razoabilidade, os dados proprietários dos não proprietários. De fato, os dados anonimizados devem ser excluídos do âmbito de aplicação da lei quando a re-identificação seja possível tão

somente através de esforços “extraordinários”, isto é, não razoáveis. Mesmo naqueles casos onde a re-identificação possa ocorrer através de esforços meramente “razoáveis”, os dados ainda deveriam ser considerados anônimos e fora da abrangência da lei se a anonimização se der com base proteções legais, obrigacionais e administrativas, como por exemplo proibições contratuais e regulatórias de re-identificar dados exceto em circunstâncias específicas.

15. Nesse sentido, a proposta abaixo:

Dados anônimos: *dados relativos a um titular que não possa ser identificado no nível individual pelo responsável pelo tratamento, tendo em conta o conjunto de meios suscetíveis de serem razoavelmente utilizados para identificar o referido titular, ou desde que os responsáveis pelo tratamento estejam sob obrigação contratual, administrativa ou legal de manter os dados anonimizados.*

II. 2 Forma de consentimento

16. A definição das modalidades e situações que exigem consentimento expresso e prévio é um dos temas em destaque no desafio de construir uma lei geral de proteção de dados assertiva e duradoura. Nesse sentido é louvável a exclusão da atual redação do Projeto de Lei 5276/16 da palavra “expressa” a qual vinha sendo apontada como uma preocupação pelas empresas (muito embora, no entender da ABRANET, deveria ser defendida por toda a sociedade digital), por possibilitar a interpretação de que a cada novo uso ou coleta de dados um novo consentimento deveria ser fornecido, o que, se de um lado, pioraria muito, ou quase inviabilizaria, a experiência do usuário na internet, de outro criaria uma artificialidade de compreensão do ambiente tecnológico pelos usuários de internet, que seria apenas formal.

17. Nesse sentido, a ABRANET reafirma seu entendimento de que o ambiente de tratamento de dados contemporâneo torna essencial que se reconheça a capacidade do titular de dados pessoais de consentir de diversas formas, sem que a necessidade de fazê-lo de maneira expressa seja mandatória a qualquer situação.

18. Também é louvável que o projeto de lei tenha prestigiado a noção de consentimento “inequívoco”, visto que a regra geral de consentimento é de que, quando necessário, ele

seja perceptível independente da forma que tenha ocorrido. O consentimento expresso ficaria, então, adstrito a casos específicos, como o tratamento de dados sensíveis. Dessa forma, sugerimos a adoção do seguinte conceito:

Consentimento: manifestação inequívoca realizada pelo titular de dados de maneira livre e informada para autorização do tratamento de seus dados pessoais.

19. Vale destacar que embora o consentimento seja um elemento importante na definição de um sistema robusto de proteção de dados, ele não deve ser a principal ferramenta que assegure ao titular dos dados uma tutela efetiva. Garantias principiológicas, com especial destaque para as relacionadas à transparência e ao controle dos titulares sobre seus dados e a observância dos princípios estabelecidos na lei, geram um ambiente de proteção que deve equilibrar o interesse do titular dos dados em tê-los preservados com práticas que são razoáveis e que cujo desenvolvimento implica no desenvolvimento de uma economia digital.
20. Ao se exigir o consentimento “expresso”, corre-se o risco de que o mesmo venha a ser por vezes impossível ou mesmo ilusório, especialmente com o desenvolvimento de tecnologias como a computação em nuvem, o tratamento de grandes volumes de dados (big data) e a chamada Internet das Coisas.
21. Na visão da ABRANET, uma forma mais eficaz de se gerar um ambiente no qual a boa-fé é tida como condição para o tratamento de dados é inserir, dentre as hipóteses em que o consentimento é dispensado, o reconhecimento das situações nas quais existe um “interesse legítimo” para que o tratamento ocorra.
22. Além disso, uma lei sobre proteção de dados seria amplamente aplicável no país, atingindo o tratamento de dados pessoais feito seja por pessoa natural, seja por pessoa jurídica de direito público ou privado (art. 1º), sejam os dados coletados por meios físicos, digitais ou por meio do uso da Internet. Mas o Marco Civil da Internet poderia vir a ser interpretado como lei específica no que diz respeito ao tratamento de dados mediante o uso da Internet no Brasil e, com base nisso, alguns poderiam argumentar pela prevalência da regra do consentimento expresso do art. 7º, VII e IX do Marco Civil, dada a sua especificidade no caso do tratamento de dados realizados mediante o uso da Internet.

23. Essa interpretação poderia levar a uma situação absurda em que o consentimento necessário para o tratamento de dados feito mediante o meio mais dinâmico e propenso à inovação, como é a Internet, seria mais rígido (livre, informado e expresso, devendo necessariamente ocorrer de forma destacada das demais cláusulas contratuais, conforme o art. 7º, VII e IX do Marco Civil da Internet) do que o exigível para o tratamento de dados por outros meios (livre, informado e inequívoco, podendo ser fornecido não só por escrito como por qualquer outro meio que o certifique, com base no art. 9º do PL 5275/2016).
24. Assim, para maior segurança jurídica e alinhamento desse regime de consentimento, sugerimos que seja acrescida uma disposição legal para alterar o artigo 7º, IX do Marco Civil, passando a consagrar a regra geral do consentimento inequívoco também no Marco Civil da Internet, nos seguintes termos:

“Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: IX - consentimento inequívoco sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais”.

II. 3 Reconhecimento do “legítimo interesse”

24. Excessos na exigência do consentimento podem resultar, muitas vezes, na chamada fadiga do consentimento, tornando o ato menos consciente e, portanto, pouco eficaz. Assim, a ABRANET considera louvável a inclusão no PL 5276/16 dos dispositivos abaixo transcritos que reconhecem a dispensa do consentimento baseada no legítimo interesse do responsável pelo tratamento:

*“Art. 7º. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
[...]*

IX – quando necessário para atender aos interesses legítimos do responsável ou de terceiro, exceto no caso de prevalecerem interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for menor de idade.”

E

“Art. 10. O legítimo interesse do responsável somente poderá fundamentar um tratamento de dados pessoais quando necessário e baseado em uma situação concreta, respeitados os direitos e liberdades fundamentais do titular.

§ 1º O legítimo interesse deverá contemplar as legítimas expectativas do titular quanto ao tratamento de seus dados, de acordo com o disposto no art. 6º, II.

§2º O responsável deverá adotar medidas para garantir a transparência do tratamento de dados baseada no seu legítimo interesse, devendo fornecer aos titulares mecanismos eficazes para que possam manifestar sua oposição ao tratamento de dados pessoais.

§ 3º Quanto o tratamento for baseado no legítimo interesse do responsável, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados, devendo ser anonimizados sempre que compatível com a finalidade do tratamento.

§ 4º O órgão competente poderá solicitar ao responsável relatório de impacto à privacidade quando o tratamento tiver como fundamento o seu legítimo interesse.

25. O reconhecimento do legítimo interesse do responsável como forma de consentimento é uma importante disposição legal para garantir que o tratamento de dados tenha como pressuposto de legitimidade a boa-fé em prol do usuário, o que lhe confere prerrogativas substanciais e superiores se comparadas com um simples clique. Da mesma forma, o conceito é essencial para a inovação, que deve sempre ocorrer em linha com os princípios da lei, permitindo assim um ambiente regulatório protetivo dos titulares de dados e aberto à realização de experiências inovadoras.

26. Ademais, com base nas discussões em curso atualmente na Europa, vale lembrar que o Working Party do Artigo 29 recentemente divulgou opinião na qual esclarece alguns critérios para se testar o que poderia ser enquadrado como interesse legítimo. Dentre os critérios adicionados pelo Working Party estão considerações sobre:

- (i) a natureza do legítimo interesse e se o tratamento é necessário para o exercício de direitos fundamentais, atende ao interesse público ou é reconhecido pela comunidade como pertinente;
- (ii) o impacto no titular dos dados e a sua razoável expectativa sobre o que acontecerá com os seus dados, bem como a natureza dos dados e como os mesmos serão processados;
- (iii) o relacionamento do responsável com o titular, que contribui na delimitação de expectativas; e
- (iv) proteções adicionais que poderiam limitar impactos indevidos no titular dos dados, como a implementação de tecnologias que sejam amigáveis à privacidade, transparência crescente no tratamento, mecanismos de opt-out sem condicionantes e portabilidade dos dados.

II. 4 Aplicação ao Estado e proteção dos direitos fundamentais do titular

27. Um tema importante identificado nos debates legislativos é a possível discrepância na aplicação de hipóteses de exceção ao consentimento do titular de dados aplicáveis a entidades privadas e entidades públicas. O entendimento da ABRANET é que a tutela do direito individual diante do Estado é tão importante quanto diante de entes privados, ou até maior, em vista da enorme capacidade do Estado em interferir na vida privada do cidadão.
28. Da mesma forma, tendo em vista a necessidade constitucional de proteção do indivíduo, suas liberdades e direitos de personalidade, que incidem não apenas nas suas relações privadas, mas também nas com o Poder Público e Estado, a ABRANET se posiciona de forma contrária a qualquer disposição que dê margem à realização de atividades de vigilância pelo Estado sobre os indivíduos ou a sua interferência na autodeterminação dos indivíduos.
29. Desta forma, a ABRANET considera salutar a inserção no texto do PL 5276/16 de capítulo específico (Capítulo IV) para disciplinar o Tratamento de Dados Pessoas pelo Poder Público, com dispositivos como o art. 23 que limita o tratamento de dados pelas pessoas jurídicas de poder público ao *“atendimento de sua finalidade pública, na persecução de um interesse público, tendo por objetivo a execução de competências legais ou cumprimento de atribuição legal pelo serviço público”*. No mesmo sentido, também são louváveis, os dispositivos que estabelecem a obrigação dos órgãos do Poder Público informarem/darem publicidade as hipóteses em que realiza o tratamento de dados; o reconhecimento da equivalência no tratamento dispensado às empresas públicas e as sociedades de economia mista que atuem em regime de concorrência com aquele dispensado às pessoas jurídicas de direito privado, particulares, entre outras.³

³ Vide redação proposta pelos os artigos 23 à 32 do PL 5276/16:

Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referenciadas no parágrafo único do art. 1º da Lei 12.527, de 18 de novembro de 2011, deverá ser realizado para o atendimento de sua finalidade pública, na persecução de um interesse público, tendo por objetivo a execução de competências legais ou o cumprimento de atribuições legal pelo serviço público.

Art. 24. Os órgãos do Poder Público deverão informar as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre essas atividades em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos.

§ 1º Os órgãos do Poder Público que realizarem operações de tratamento de dados pessoais deverão indicar um encarregado, nos termos do art. 40.

§ 2º O órgão competente poderá dispor sobre as formas pelas quais se dará a publicidade das operações de tratamento.

Art. 25. As empresas públicas e as sociedades de economia mista que atuem em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei. Parágrafo único. As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e não estiverem atuando em regime de concorrência, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos desse Capítulo.

30. Ademais, vale ressaltar as preocupações com possíveis dispositivos que afrontem direitos fundamentais do cidadão, como a liberdade de expressão e o acesso à informação. Por exemplo, o direito a requerer a dissociação, bloqueio ou cancelamento de dados desnecessários ou excessivos, ou mesmo a possibilidade de requerer a correção de dados inexatos, pode resultar em pedidos de modificação de informações que reflitam opinião ou que sejam importantes e válidas no contexto de informação pública. Assim, o cancelamento dos dados a partir do requerimento do titular ou pelo término do tratamento não pode ser um direito absoluto ou dependente de consentimento, tendo em vista que o responsável tem, por força de inúmeras leis, obrigações de conservação de dados, que podem ser incompatíveis com essas orientações.

II. 5 Segredo Industrial.

31. Para proteger o sigilo das informações industriais, a ABRANET sugere a esta D. Comissão que acrescente a exceção da proteção ao segredo empresarial nos artigos 10, § 4º, 13, § 3º, 19 e 20.

II. 6 Transferência internacional de dados

Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios da proteção de dados pessoais elencados no art. 6º desta Lei.

Parágrafo único. É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto em casos de execução descentralizada de atividade pública que o exija e exclusivamente para este fim específico e determinado, observando o disposto na Lei nº 12.527 de 2011.

Art. 27. A comunicação e a transferência de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informada ao órgão competente e dependerá de consentimento do titular, exceto:

I- Nas hipóteses de dispensa de consentimento prevista nesta Lei; ou:

II- Nos casos de uso compartilhado de dados, em que será dada publicidade nos termos art. 24.

Art. 28. A comunicação de dados pessoais entre órgãos e entidades de direito público será objeto de publicidade, nos termos art. 24.

Art. 29. O órgão competente poderá solicitar, a qualquer momento, às entidades do Poder Público a realização de operações de tratamento de dados pessoais, informe específico sobre o âmbito, natureza dos dados e demais detalhes do tratamento realizado, podendo emitir parecer técnico complementar para garantir o cumprimento desta Lei.

Art. 30. O órgão competente poderá estabelecer normas complementares para as atividades de comunicação de dados pessoais.

Art. 31. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, o órgão competente poderá enviar informe com medidas cabíveis para fazer cessar a violação.

Parágrafo único. As punições cabíveis a agente público no âmbito desta Lei serão aplicadas pessoalmente aos operadores de órgãos públicos, conforme disposto na Lei nº 8.112, de 11 de dezembro de 1990, e na Lei nº 8.429, de 2 de junho de 1992.

Art. 32. O órgão competente poderá solicitar a agentes do poder público a publicação de relatórios de impacto de privacidade e poderá sugerir a adoção de padrões e boas práticas aos tratamentos de dados pessoais pelo poder público.

Associação Brasileira de Internet

Rua da Quitanda, 96 – cj 31 - CEP: 01012-010 – São Paulo – SP - Tel./Fax: (11) 3078-3866

www.abranet.org.br

32. A ABRANET sugere uma reflexão sobre a adoção de modelo brasileiro que possa efetivamente garantir segurança e respeito aos direitos dos titulares ao obrigar o responsável pelo tratamento, independentemente de onde os dados pessoais sejam tratados. O importante é a responsabilidade do responsável diante do titular. A ABRANET observa, ainda, ao se definir as hipóteses em que a transferência internacional pode ser feita, independente do equivalente nível de proteção do país receptor de dados, deve-se incluir uma exceção específica para pessoas jurídicas pertencentes ao mesmo grupo econômico.

33. Além disso, a hipótese de transferência internacional mediante consentimento específico para essa finalidade deve ser reconhecida, porém deve ser excluída a obrigação de que seja apresentada informação sobre riscos envolvidos e detalhamento de vulnerabilidades do país de destino resulta em dados subjetivos, pois na prática esta inviabilizaria a hipótese de transferência mediante consentimento, afrontando a vontade do próprio titular dos dados. Desta forma, sugere-se a supressão da parte final do texto proposto no inciso VII do art. 33 do PL 5276:

~~"VII - quando o titular tiver fornecido o seu consentimento para a transferência, com informação prévia e específica sobre o caráter internacional da operação, com alerta quanto aos riscos envolvidos."~~

34. A ABRANET entende, ainda, que é essencial previsão de bases legais amplas para as transferências internacionais de dados, com o reconhecimento de uma série de mecanismos legítimos para além da regra da adequação e do consentimento, incluindo o cumprimento de compromissos assumidos em acordos de cooperação internacional e a tutela da vida e da incolumidade física dos titulares, dentre outros aspectos, já louvadamente previstos no PL 5276. É especialmente bem-vinda a incorporação de mecanismos amplamente aceitos como as "cláusulas contratuais padrão", "padrões corporativos globais" e "regras corporativas globais" (conhecidos na Europa como "Binding Corporate Rules" ou "BCRs"), posicionando o Brasil no cenário das transferências internacionais de dados.

35. Contudo, mesmo as cláusulas contratuais padrão e as normas corporativas globais têm as suas limitações: as primeiras não são flexíveis e podem resultar em complexidades indesejáveis, e as últimas limitam-se a transferências dentro de um grupo corporativo. Assim, para que o Capítulo sobre a Transferência Internacional de Dados do PL 5276 seja

ainda mais aprimorada e ecoe ainda mais a natureza global dos fluxos de dados modernos e das atividades econômicas a ele atreladas, o art. 33 deve incluir a previsão de mecanismos como selos, certificados e códigos de conduta organizacionais emitidos por terceiros qualificados e aprovados pela autoridade competente — são opções já disponíveis em outras jurisdições, com o benefício de não se limitarem às transferências dentro de um mesmo grupo corporativo.

36. Um exemplo marcante da adoção desses mecanismos é o sistema do *Cross-Border Privacy Rule* (CBPR), desenvolvido e adotado no âmbito do Foro de Cooperação Econômica Ásia-Pacífico (APEC), e as certificações da União Europeia, no âmbito do GDPR, ambos com o objetivo de assegurar mecanismos de transferência de dados que permitam transferências não apenas dentro de um mesmo grupo corporativo global, mas também entre empresas não afiliadas.
37. O México também está dando passos nesse mesmo sentido e recentemente colocou em prática um mecanismo de auto-regulação com o objetivo de se compatibilizar com o sistema CBPR e permitir fluxos de dados ainda mais seguros e confiáveis⁴.
38. Selos, certificados e códigos de conduta internacionalmente reconhecidos apoiam as transferências internacionais de dados e estimulam que elas se deem com responsabilidade e transparência.
39. No que diz respeito ao requisito do projeto de que apenas o "órgão competente" autorize essas regras corporativas ou códigos de conduta globais, sugerimos que seja modificado para estimular que o próprio órgão competente (1) desenvolva "cláusulas padrão" cuja adoção independa de autorização específica; (2) reconheça regras e códigos internacionalmente aceitos sem a necessidade de autorização específica; e (3) permita que organismos de certificação reconhecidos prevejam essas regras corporativas ou códigos de conduta globais, bem como aprovem e atestem a adequação das organizações a eles, de maneira semelhante ao papel desempenhado pelos chamados *Accountability Agents* no sistema APEC CBPR e de modo a evitar gargalos de aprovação no âmbito das autoridades competentes.
40. Não é realista nem desejável impor ao órgão competente um volume desproporcional de processos administrativos para a aprovação específica de transferências internacionais

⁴ http://www.dof.gob.mx/nota_detalle.php?codigo=5346597&fecha=29/05/2014.

de dados — esses processos de aprovação prévia e específica devem, na verdade, ser reduzidos ao mínimo necessário e reservados aos casos excepcionais que efetivamente demandem a atenção do órgão competente. Se assim não for, o órgão competente teria que alocar praticamente a totalidade de seu tempo produtivo para analisar pedidos e processos de aprovação de transferências de dados, o que, definitivamente, não implicaria uma atuação mais estratégica do órgão, muito menos níveis de proteção significativamente maiores para os titulares dos dados.

41. Vale ressaltar que o Foro de Cooperação Econômica Ásia-Pacífico e a União Europeia têm explorado maneiras de racionalizar os processos de certificação e aprovação de empresas que procuram a "dupla certificação" nos dois sistemas, assim como têm explorado formas de tornar as novas certificações com relação à GDPR compatíveis e interoperáveis em relação à CBPR. Tendo em vista essa tendência, os mecanismos sobre transferência internacional de dados previstos na lei brasileira devem desde já ser projetados de modo a que também sejam interoperáveis em relação a estes e outros sistemas de cooperação similares para transferências internacionais, para garantir que as empresas que tenham recebido aprovação sob um sistema não brasileiro possam alavancar sua aprovação no Brasil e vice-versa.

42. Com base nessas considerações, sugerimos as seguintes emendas adicionais ao Capítulo sobre a Transferência Internacional de Dados do PL 5276:

*"Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
I - para países que proporcionem nível de proteção de dados pessoais ao menos equiparável ao desta Lei;*

II - quando a transferência for necessária para a cooperação judicial internacional entre órgãos públicos de inteligência e de investigação, de acordo com os instrumentos de direito internacional;

III - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

IV - quando o órgão competente autorizar a transferência;

V - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

VI - quando a transferência for necessária para execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do art. 24; ou

VII - quando o titular tiver fornecido o seu consentimento para a transferência, com informação prévia e específica sobre o caráter internacional da operação, com alerta quanto aos riscos envolvidos.

VIII - quando o responsável pelo tratamento comprovar que a transferência se baseia em cláusulas contratuais padrão aprovadas pelo órgão competente ou em regras e códigos internacionalmente aceitos;

IX - quando o responsável pelo tratamento comprovar que detém selos, certificados ou códigos de conduta e adequação emitidos por organismos de certificação qualificados e aprovados pelo órgão competente.

Parágrafo único. O nível de proteção de dados do país estrangeiro será avaliado pelo órgão competente, que levará em conta:

I - as normas gerais e setoriais da legislação em vigor no país de destino;

II - a natureza dos dados;

III - a observância dos princípios gerais de proteção de dados pessoais previstos nesta Lei;

IV - a adoção de medidas de segurança previstas em regulamento;

V - as outras circunstâncias específicas relativas à transferência.

Art. 34. A autorização referida no inciso IV do caput do art. 33 será concedida quando o responsável pelo tratamento apresentar garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular **e será dispensável nas hipóteses dos incisos VIII e IX do art. 33 desta Lei, apresentadas em cláusulas contratuais aprovadas pelo órgão competente para uma transferência específica, em cláusulas contratuais padrão ou em normas corporativas globais, nos termos do regulamento.**

§1º O órgão competente poderá elaborar cláusulas contratuais padrão ou homologar dispositivos constantes em documentos que fundamentem a transferência internacional de dados, que deverão observar os princípios gerais de proteção de dados e os direitos do titular, garantida a responsabilidade solidária do cedente e do cessionário, independentemente de culpa.

§2º Os responsáveis pelo tratamento que fizerem parte de um mesmo grupo econômico ou conglomerado multinacional poderão submeter normas corporativas globais à aprovação do órgão competente, obrigatórias para todas as empresas integrantes do grupo ou do conglomerado, a fim de obter permissão para transferências internacionais de dados dentro do grupo ou do conglomerado sem necessidade de autorizações específicas, observados os princípios gerais de proteção e os direitos do titular.

§3º Na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação do órgão competente, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento.

§4º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no caput serão, também, analisadas de acordo com o previsto nos §1º e §2º do art. 45".

II. 7 Autoridade competente

43. Outro tema que permeia o debate legislativo é a criação de uma "autoridade competente" para regular o tratamento de dados pessoais. Verificamos que na atual redação do artigo 53 do PL 5276/16 apresenta uma previsão expressa para a criação de um "órgão competente" com as seguintes competências:

Art. 53. O órgão competente designado para zelar pela implementação e pela fiscalização desta Lei terá as seguintes atribuições:

I- Zelar pela proteção dos dados pessoais, nos termos da legislação;

II- Elaborar diretrizes para um Política Nacional de Proteção de Dados Pessoais e Privacidade;

III- Realizar auditoria nos tratamentos de dados pessoais e processos envolvidos com dados pessoais visando garantir a sua conformidade aos princípios e regras desta Lei;

IV- Promover entre a população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e as medidas de segurança;

V- Promover estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;

VI- Estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais.

VII- Promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transacional;

VIII- Dispor sobre as formas pelas quais se dará a publicidade das operações de tratamento;

IX- Solicitar, a qualquer momento, às entidades do Poder Público que realizem operações de tratamento de dados pessoais, informe específico sobre o âmbito, natureza dos dados e demais detalhes de tratamento realizado, podendo emitir parecer técnico complementar para garantir o cumprimento desta Lei;

X- Estabelecer normas complementares para as atividades de comunicação de dados pessoais;

XI- Elaborar relatórios anuais acerca de suas atividades;

XII- Editar normas sobre proteção de dados pessoais e privacidade; e

XIII- Realizar demais ações dentro de sua esfera de competência, inclusive as previstas nesta Lei e em legislação específica.

44. Se a opção do legislador for pela existência de autoridade, a ABRANET ressalta que deve existir uma estrutura autônoma, que seja neutra e equidistante para avaliar a observância da lei de proteção dos dados, com independência e orçamento próprio, desvinculado de eventuais sanções pecuniárias que venham a ser aplicadas pela entidade e que de acordo com os princípios do Estado Democrático de Direito tenha a sua atuação restrita pela expressão "*de acordo com os limites e princípios previstos na presente lei*". Em suma, a ABRANET sugere que a estruturação de uma eventual autoridade seja pautada pelos seguintes aspectos:

- (i) membros escolhidos com base em múltiplas visões das questões de privacidade, com formação técnica prevalecendo sobre a política;
- (ii) capacidade de análise holística da proteção de dados, levando em conta os impactos na inovação, na economia, nas relações empresariais, internacionais e de consumo, e nas questões concorrenciais; e
- (iii) autonomia e orçamento próprio, desvinculado de eventuais sanções pecuniárias que venham a ser aplicadas pela entidade.
- (iv) limitação de discricionariedade e sistema de freios e contrapesos, notadamente para evitar impactos em sigilo e governança.

45. Ademais, tendo em vista a pluralidade de interesses envolvidos no tratamento de dados, seria interessante considerar a hipótese de criação de um conselho consultivo multisetorial, como instância de apoio às decisões da referida autoridade de proteção de dados, enriquecendo-as com a contribuição dos mais distintos setores interessados. Uma solução multisetorial interessante foi a criada pelo art. 54 do PL 5.276/16⁵, o qual trouxe

⁵ Art. 54. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto por quinze representantes titulares, e seus respectivos suplentes, dos seguintes órgãos:

em sua redação a proposta de criação de um Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, um conselho que terá em seus quadros entre outros um representante da sociedade civil, um da academia e dois do setor privado. Este Conselho terá as seguintes competências:

Art.55 Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade:

- I - fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade;*
- II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade;*
- III - sugerir ações a serem realizadas pelo órgão competente;*
- IV - realizar estudos e debates sobre a proteção de dados pessoais e da privacidade; e*
- V - disseminar o conhecimento sobre proteção de dados pessoais e privacidade à população em geral.*

II.8 Vacatio legis

46. A ABRANET entende que as mudanças propostas PL impactam profundamente o dia-a-dia da população brasileira e, principalmente, das empresas que atuam no Brasil. Assim, é preciso garantir uma vacatio legis proporcional para que a sociedade tenha tempo de assimilar todas as alterações promovidas pelo novo marco legal. Nesse sentido a sugestão abaixo:

“Art. 56. Esta Lei entrará em vigor ~~cento e oitenta dias após a~~ no prazo de 3 (três) anos contados da data da sua publicação.”

Conclusão

47. Como visto ao longo desta manifestação, a ABRANET entende que é de grande importância o reconhecimento de que o tratamento de dados é benéfico, quando realizado

-
- I- Sete representantes do Poder Executivo federal*
 - II- Um representante indicado pelo Congresso Nacional;*
 - III- Um representante indicado pelo Conselho Nacional de Justiça;*
 - IV- Um representante indicado pelo Conselho Nacional do Ministério Público;*
 - V- Um representante indicado pelo Comitê Gestor da Internet do Brasil;*
 - VI- Um representante da sociedade civil;*
 - VII- Um representante da academia; e*
 - VIII- Dois representantes do setor privado*

§ 1º Os representantes serão designados por ato do Ministro de Estado da Justiça e terão mandato de dois anos, permitida uma recondução.

Associação Brasileira de Internet

Rua da Quitanda, 96 – cj 31 - CEP: 01012-010 – São Paulo – SP - Tel./Fax: (11) 3078-3866

www.abranet.org.br

em conformidade com os princípios previstos na legislação e na Constituição Federal, sendo parte integrante do processo de inovação e evolução da sociedade. Por isso é imperativo que qualquer iniciativa legislativa tenha como norte a proteção adequada dos dados dos cidadãos sem engessar ou condenar as atividades econômicas a eles associadas.

48. Por fim, a ABRANET apresenta o quadro anexo, no qual suas principais sugestões e comentários à atual redação do PL 5276/16 encontram-se consolidados de forma mais sistemática.

Sendo o que nos cabia para o momento, renovamos nossos votos de estima e consideração.

São Paulo, 23 de junho de 2017

Abranet - Associação Brasileira de Internet
Por seu presidente, Eduardo Fumes Parajo

QUADRO ANEXO

Tema	PL 5276/2016	Visão ABRANET
1. Conceitos de “Dado Pessoal” e “Dados Anônimos”	<p><u>Art. 5º. I</u></p> <p><i>“I – dado pessoal: dado relacionado à pessoa natural identificada ou identificável, inclusive números identificados, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa.”</i></p>	<p><u>Comentário:</u></p> <p>A ABRANET entende que o conceito de “dado pessoal” merece uma definição pragmática, calcada na probabilidade de o dado efetivamente levar à identificação de um indivíduo determinado, em outras palavras a definição de “dado pessoal” deve estar relacionada a uma pessoa identificada ou identificável no nível individual. Neste sentido, apresenta-se a seguinte sugestão de redação:</p> <p><u>Sugestão de redação:</u></p> <p><i>“Dado pessoal: dado relacionado à pessoa natural identificada ou identificável no nível individual.”</i></p>
	<p><u>Art. 5º. IV</u></p> <p><i>“IV – dados anonimizados: dados relativos a um titular que não possa ser identificado.”</i></p>	<p><u>Comentário:</u></p> <p>Com relação ao termo “dado anônimo”, para que se vença o desafio regulatório supra mencionado, ou seja, ao mesmo tempo que seja tutelado o dado pessoal, proteja-se a florescência de economia de dados e, principalmente, sejam criados parâmetros de legitimidade para o trabalho das empresas sérias com dados que não levem à identificação de pessoas sem esforços razoáveis, é igualmente importante que seu conceito seja assertivo.</p> <p>Do ponto de vista jurídico, se está diante de situação de graus distintos de proteção, necessários, ademais, para que se possa impulsionar um ambiente institucional que favoreça o respeito à proteção efetiva dos dados pessoais, separando, com razoabilidade,</p>

Tema	PL 5276/2016	Visão ABRANET
		<p>os dados proprietários dos não proprietários. De fato, os dados anonimizados devem ser excluídos do âmbito de aplicação da lei quando a re-identificação seja possível tão somente através de esforços “extraordinários”, isto é, não razoáveis. Mesmo naqueles casos onde a re-identificação possa ocorrer através de esforços meramente “razoáveis”, os dados ainda deveriam ser considerados anônimos e fora da abrangência da lei se a anonimização se der com base proteções legais, obrigacionais e administrativas, como por exemplo proibições contratuais e regulatórias de re-identificar dados exceto em circunstâncias específicas. Nesse sentido, a proposta abaixo:</p> <p><u>Sugestão de redação:</u></p> <p><i>“Dados anônimos: dados relativos a um titular que não possa ser identificado no nível individual pelo responsável pelo tratamento, tendo em conta o conjunto de meios suscetíveis de serem razoavelmente utilizados para identificar o referido titular, <u>ou desde que os responsáveis pelo tratamento estejam sob obrigação contratual, administrativa ou legal de manter os dados anonimizados.</u>”</i></p>
<p>2. Forma de consentimento</p>	<p><u>Art. 5º. VII</u></p> <p><i>VII – consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.</i></p> <p><u>Art. 7º. I</u></p> <p><i>Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:</i> <i>I – mediante o fornecimento pelo titular de consentimento, livre, informado e inequívoco.</i></p>	<p><u>Comentário 1:</u></p> <p>A definição das modalidades e situações que exigem consentimento expresso e prévio é um dos temas em destaque no desafio de construir uma lei geral de proteção de dados assertiva e duradoura. Nesse sentido é louvável a exclusão da atual redação do Projeto de Lei 5276/13 da palavra “expressa” a qual vinha sendo apontada como uma preocupação pelas empresas (muito embora, no entender da ABRANET, deveria ser defendida por toda a sociedade digital), por possibilitar a interpretação de que a cada novo uso ou coleta de dados um novo consentimento deveria ser fornecido, o que, se de um lado, pioraria muito, ou quase inviabilizaria, a experiência do usuário na internet, de outro criaria uma artificialidade de compreensão do ambiente tecnológico pelos usuários de internet, que seria apenas formal.</p>

Tema	PL 5276/2016	Visão ABRANET
		<p>Nesse sentido, a ABRANET reafirma seu entendimento de que o ambiente de tratamento de dados contemporâneo torna essencial que se reconheça a capacidade do titular de dados pessoais de consentir de diversas formas, sem que a necessidade de fazê-lo de maneira expressa seja mandatória a qualquer situação.</p> <p>Também é louvável que o projeto de lei tenha prestigiado a noção de consentimento “inequívoco”, visto que a regra geral de consentimento é de que, quando necessário, ele seja perceptível independente da forma que tenha ocorrido. O consentimento expresso ficaria, então, adstrito a casos específicos, como o tratamento de dados sensíveis. Dessa forma, sugerimos a adoção do seguinte conceito:</p> <p><u>Sugestão de redação 1:</u></p> <p><i>“Consentimento: manifestação inequívoca realizada pelo titular de dados de maneira livre e informada para autorização do tratamento de seus dados pessoais.”</i></p> <p><u>Comentário 2:</u></p> <p>Para maior segurança jurídica e alinhamento desse regime de consentimento, sugerimos que seja acrescida uma disposição legal para alterar o artigo 7º, IX do Marco Civil, passando a consagrar a regra geral do consentimento inequívoco também no Marco Civil da Internet, nos seguintes termos:</p> <p><u>Sugestão de redação 2:</u></p> <p><i>Marco Civil da Internet “Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: IX - consentimento inequívoco sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais”.</i></p>

Tema	PL 5276/2016	Visão ABRANET
<p>3. Reconhecimento do “legítimo interesse”</p>	<p><u>Art. 7º, IX.</u></p> <p><i>Art. 7º. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:</i></p> <p><i>[...]</i></p> <p><i>IX – quando necessário para atender aos interesses legítimos do responsável ou de terceiro, exceto no caso de prevalecerem interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for menor de idade.</i></p> <p><u>Art. 10.</u></p> <p><i>Art. 10. O legítimo interesse do responsável somente poderá fundamentar um tratamento de dados pessoais quando necessário e baseado em uma situação concreta, respeitados os direitos e liberdades fundamentais do titular.</i></p> <p><i>§ 1º O legítimo interesse deverá contemplar as legítimas expectativas do titular quanto ao tratamento de seus dados, de acordo com o disposto no art. 6º, II.</i></p> <p><i>§2º O responsável deverá adotar medidas para garantir a transparência do tratamento de dados</i></p>	<p><u>Comentário:</u></p> <p>Excessos na exigência do consentimento podem resultar, muitas vezes, na chamada fadiga do consentimento, tornando o ato menos consciente e, portanto, pouco eficaz. Assim, a ABRANET considera louvável a inclusão no PL 5276/16 dos dispositivos transcritos que reconhecem a dispensa do consentimento baseada no legítimo interesse do responsável pelo tratamento.</p>

Tema	PL 5276/2016	Visão ABRANET
	<p><i>baseada no seu legítimo interesse, devendo fornecer aos titulares mecanismos eficazes para que possam manifestar sua oposição ao tratamento de dados pessoais.</i></p> <p><i>§ 3º Quanto o tratamento for baseado no legítimo interesse do responsável, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados, devendo ser anonimizados sempre que compatível com a finalidade do tratamento.</i></p> <p><i>§ 4º O órgão competente poderá solicitar ao responsável relatório de impacto à privacidade quando o tratamento tiver como fundamento o seu legítimo interesse.</i></p>	
<p>4. Aplicação ao Estado e proteção dos direitos fundamentais do titular</p>	<p><i>Seção I – Tratamento de Dados Pessoais pelo Poder Público</i></p> <p><i>Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referenciadas no parágrafo único do art. 1º da Lei 12.527, de 18 de novembro de 2011, deverá ser realizado para o atendimento de sua finalidade pública, na persecução de um interesse público, tendo por objetivo a execução de competências legais ou o cumprimento de atribuições legal pelo serviço público.</i></p>	<p><u>Comentário:</u></p> <p>Um tema importante identificado nos debates legislativos é a possível discrepância na aplicação de hipóteses de exceção ao consentimento do titular de dados aplicáveis a entidades privadas e entidades públicas. O entendimento da ABRANET é que a tutela do direito individual diante do Estado é tão importante quanto diante de entes privados, ou até maior, em vista da enorme capacidade do Estado em interferir na vida privada do cidadão.</p> <p>Da mesma forma, tendo em vista a necessidade constitucional de proteção do indivíduo, suas liberdades e direitos de personalidade, que incidem não apenas nas suas relações privadas, mas também nas com o Poder Público e Estado, a ABRANET se posiciona de forma contrária a qualquer disposição que dê margem à realização de atividades de vigilância pelo Estado sobre os indivíduos ou a sua interferência na autodeterminação dos indivíduos.</p>

Tema	PL 5276/2016	Visão ABRANET
	<p><i>Art. 24. Os órgãos do Poder Público deverão informar as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre essas atividades em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos.</i></p> <p><i>§ 1º Os órgãos do Poder Público que realizarem operações de tratamento de dados pessoais deverão indicar um encarregado, nos termos do art. 40.</i></p> <p><i>§ 2º O órgão competente poderá dispor sobre as formas pelas quais se dará a publicidade das operações de tratamento.</i></p> <p><i>Art. 25. As empresas públicas e as sociedades de economia mista que atuem em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.</i></p> <p><i>Parágrafo único. As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e não estiverem atuando em regime de concorrência, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos desse Capítulo.</i></p>	<p>Desta forma, a ABRANET considera salutar a inserção no texto do PL 5276/16 de capítulo específico (Capítulo IV) para disciplinar o Tratamento de Dados Pessoais pelo Poder Público, com dispositivos como o art. 23 que limita o tratamento de dados pelas pessoas jurídicas de poder público ao “<i>atendimento de sua finalidade pública, na persecução de um interesse público, tendo por objetivo a execução de competências legais ou cumprimento de atribuição legal pelo serviço público</i>”. No mesmo sentido, também são louváveis, os dispositivos que estabelecem a obrigação dos órgãos do Poder Público informarem/darem publicidade as hipóteses em que realiza o tratamento de dados; o reconhecimento da equivalência no tratamento dispensado às empresas públicas e as sociedades de economia mista que atuem em regime de concorrência com aquele dispensado às pessoas jurídicas de direito privado, particulares, entre outras.</p> <p>Ademais, vale ressaltar as preocupações com possíveis dispositivos que afrontem direitos fundamentais do cidadão, como a liberdade de expressão e o acesso à informação. Por exemplo, o direito a requerer a dissociação, bloqueio ou cancelamento de dados desnecessários ou excessivos, ou mesmo a possibilidade de requerer a correção de dados inexatos, pode resultar em pedidos de modificação de informações que reflitam opinião ou que sejam importantes e válidas no contexto de informação pública. Assim, o cancelamento dos dados a partir do requerimento do titular ou pelo término do tratamento não pode ser um direito absoluto ou dependente de consentimento, tendo em vista que o responsável tem, por força de inúmeras leis, obrigações de conservação de dados, que podem ser incompatíveis com essas orientações.</p>

Tema	PL 5276/2016	Visão ABRANET
	<p><i>Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios da proteção de dados pessoais elencados no art. 6º desta Lei.</i></p> <p><i>Parágrafo único. É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto em casos de execução descentralizada de atividade pública que o exija e exclusivamente para este fim específico e determinado, observando o disposto na Lei nº 12.527 de 2011.</i></p> <p><i>Art. 27. A comunicação e a transferência de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informada ao órgão competente e dependerá de consentimento do titular, exceto:</i></p> <p><i>I- Nas hipóteses de dispensa de consentimento prevista nesta Lei; ou:</i></p> <p><i>II- Nos casos de uso compartilhado de dados, em que será dada publicidade nos termos art. 24.</i></p> <p><i>Art. 28. A comunicação de dados pessoais entre órgãos e entidades de direito público será objeto de publicidade, nos termos art. 24.</i></p> <p><i>Art. 29. O órgão competente poderá solicitar, a qualquer momento, às entidades do Poder Público a</i></p>	

Tema	PL 5276/2016	Visão ABRANET
	<p><i>realização de operações de tratamento de dados pessoais, informe específico sobre o âmbito, natureza dos dados e demais detalhes do tratamento realizado, podendo emitir parecer técnico complementar para garantir o cumprimento desta Lei.</i></p> <p><i>Art. 30. O órgão competente poderá estabelecer normas complementares para as atividades de comunicação de dados pessoais.</i></p> <p><i>Seção II – Responsabilidade</i></p> <p><i>Art. 31. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, o órgão competente poderá enviar informe com medidas cabíveis para fazer cessar a violação.</i></p> <p><i>Parágrafo único. As punições cabíveis a agente público no âmbito desta Lei serão aplicadas pessoalmente aos operadores de órgãos públicos, conforme disposto na Lei nº 8.112, de 11 de dezembro de 1990, e na Lei nº 8.429, de 2 de junho de 1992.</i></p> <p><i>Art. 32. O órgão competente poderá solicitar a agentes do poder público a publicação de relatórios de impacto de privacidade e poderá sugerir a adoção de padrões e boas práticas aos tratamentos de dados pessoais pelo poder público.</i></p>	

Tema	PL 5276/2016	Visão ABRANET
5. Segredo Industrial	<i>Artigos 10, § 4º, 13, § 3º, 19 e 20.</i>	<p><u>Comentário:</u></p> <p>Para proteger o sigilo das informações industriais, a ABRANET sugere a esta D. Comissão que acrescente a exceção da proteção ao segredo empresarial em artigos 10, § 4º, 13, § 3º, 19 e 20.</p>
6. Transferência internacional de dados	<p><i>Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:</i></p> <p><i>I - para países que proporcionem nível de proteção de dados pessoais ao menos equiparável ao desta Lei;</i></p> <p><i>II - quando a transferência for necessária para a cooperação judicial internacional entre órgãos públicos de inteligência e de investigação, de acordo com os instrumentos de direito internacional;</i></p> <p><i>III - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;</i></p> <p><i>IV - quando o órgão competente autorizar a transferência;</i></p> <p><i>V - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;</i></p> <p><i>VI - quando a transferência for necessária para execução de política pública ou atribuição legal do</i></p>	<p><u>Comentário:</u></p> <p>A ABRANET sugere uma reflexão sobre a adoção de modelo brasileiro que possa efetivamente garantir segurança e respeito aos direitos dos titulares ao obrigar o responsável pelo tratamento, independentemente de onde os dados pessoais sejam tratados. O importante é a responsabilidade do responsável diante do titular. A ABRANET observa, ainda, ao se definir as hipóteses em que a transferência internacional pode ser feita, independente do equivalente nível de proteção do país receptor de dados, deve-se incluir uma exceção específica para pessoas jurídicas pertencentes ao mesmo grupo econômico.</p> <p>Além disso, a hipótese de transferência internacional mediante consentimento específico para essa finalidade deve ser reconhecida, porém deve ser excluída a obrigação de que seja apresentada informação sobre riscos envolvidos e detalhamento de vulnerabilidades do país de destino resulta em dados subjetivos, pois na prática esta inviabilizaria a hipótese de transferência mediante consentimento, afrontando a vontade do próprio titular dos dados. Desta forma, sugere-se a supressão da parte final do texto proposto no inciso VII do art. 33 do PL 5276.</p> <p>A ABRANET entende, ainda, que a adoção de cláusulas-padrão pelo responsável deveria, por si só, bastar para possibilitar a transferência internacional dos dados pessoais,</p>

Tema	PL 5276/2016	Visão ABRANET
	<p><i>serviço público, sendo dada publicidade nos termos do art. 24; ou</i></p> <p><i>VII - quando o titular tiver fornecido o seu consentimento para a transferência, com informação prévia e específica sobre o caráter internacional da operação, com alerta quanto aos riscos envolvidos.</i></p> <p><i>Parágrafo único. O nível de proteção de dados do país estrangeiro será avaliado pelo órgão competente, que levará em conta:</i></p> <p><i>I - as normas gerais e setoriais da legislação em vigor no país de destino;</i></p> <p><i>II - a natureza dos dados;</i></p> <p><i>III - a observância dos princípios gerais de proteção de dados pessoais previstos nesta Lei;</i></p> <p><i>IV - a adoção de medidas de segurança previstas em regulamento; e</i></p> <p><i>V - as outras circunstâncias específicas relativas à transferência.</i></p> <p><i>Art. 34. A autorização referida no inciso IV do caput do art. 33 será concedida quando o responsável pelo tratamento apresentar garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular, apresentadas em cláusulas contratuais aprovadas pelo órgão competente para uma transferência específica, em cláusulas contratuais padrão ou em normas corporativas globais, nos termos do regulamento.</i></p> <p><i>§ 1 O órgão competente poderá elaborar cláusulas contratuais padrão ou homologar dispositivos</i></p>	<p>independente dos outros critérios mencionados na lei. Além disso, a regra de solidariedade entre cedente e cessionário não parece razoável, uma vez que as obrigações perante o titular de dados podem ser distintas, uma vez que este pode ter consentido o tratamento com finalidades distintas para cedente e cessionário. Por isso, cada um deve ser responsável por suas obrigações respectivas perante o titular dos dados.</p> <p>A ABRANET entende, ainda, que é essencial previsão de bases legais amplas para as transferências internacionais de dados, com o reconhecimento de uma série de mecanismos legítimos para além da regra da adequação e do consentimento, incluindo o cumprimento de compromissos assumidos em acordos de cooperação internacional e a tutela da vida e da incolumidade física dos titulares, dentre outros aspectos, já louvadamente previstos no PL 5276. É especialmente bem-vinda a incorporação de mecanismos amplamente aceitos como as "cláusulas contratuais padrão", "padrões corporativos globais" e "regras corporativas globais" (conhecidos na Europa como "Binding Corporate Rules" ou "BCRs"), posicionando o Brasil no cenário das transferências internacionais de dados.</p> <p>Contudo, mesmo as cláusulas contratuais padrão e as normas corporativas globais têm as suas limitações: as primeiras não são flexíveis e podem resultar em complexidades indesejáveis, e as últimas limitam-se a transferências dentro de um grupo corporativo. Assim, para que o Capítulo sobre a Transferência Internacional de Dados do PL 5276 seja ainda mais aprimorada e ecoe ainda mais a natureza global dos fluxos de dados modernos e das atividades econômicas a ele atreladas, o art. 33 deve incluir a previsão de mecanismos como selos, certificados e códigos de conduta organizacionais emitidos por terceiros qualificados e aprovados pela autoridade competente — são opções já disponíveis em outras jurisdições, com o benefício de não se limitarem às transferências dentro de um mesmo grupo corporativo.</p> <p>Um exemplo marcante da adoção desses mecanismos é o sistema do Cross-Border Privacy Rule (CBPR), desenvolvido e adotado no âmbito do Foro de Cooperação Econômica Ásia-Pacífico (APEC), e as certificações da União Europeia, no âmbito do GDPR, ambos com o</p>

Tema	PL 5276/2016	Visão ABRANET
	<p><i>constantes em documentos que fundamentem a transferência internacional de dados, que deverão observar os princípios gerais de proteção de dados e os direitos do titular, garantida a responsabilidade solidária do cedente e do cessionário, independentemente de culpa.</i></p> <p><i>§ 2 Os responsáveis pelo tratamento que fizerem parte de um mesmo grupo econômico ou conglomerado multinacional poderão submeter normas corporativas globais à aprovação do órgão competente, obrigatórias para todas as empresas integrantes do grupo ou do conglomerado, a fim de obter permissão para transferências internacionais de dados dentro do grupo ou do conglomerado sem necessidade de autorizações específicas, observados os princípios gerais de proteção e os direitos do titular.</i></p> <p><i>§ 3 Na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação do órgão competente, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento.</i></p> <p><i>§ 4 As garantias suficientes de observância dos princípios gerais de proteção dos direitos do titular referidas no caput serão, também, analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos § 1 e § 2 do art. 45</i></p>	<p>objetivo de assegurar mecanismos de transferência de dados que permitam transferências não apenas dentro de um mesmo grupo corporativo global, mas também entre empresas não afiliadas.</p> <p>O México também está dando passos nesse mesmo sentido e recentemente colocou em prática um mecanismo de auto-regulação com o objetivo de se compatibilizar com o sistema CBPR e permitir fluxos de dados ainda mais seguros e confiáveis⁶.</p> <p>Selos, certificados e códigos de conduta internacionalmente reconhecidos apoiam as transferências internacionais de dados e estimulam que elas se deem com responsabilidade e transparência.</p> <p><u>Sugestão de redação:</u></p> <p><i>“Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:</i></p> <ul style="list-style-type: none"> <i>I - para países que proporcionem nível de proteção de dados pessoais ao menos equiparável ao desta Lei;</i> <i>II - quando a transferência for necessária para a cooperação judicial internacional entre órgãos públicos de inteligência e de investigação, de acordo com os instrumentos de direito internacional;</i> <i>III - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;</i> <i>IV - quando o órgão competente autorizar a transferência;</i> <i>V - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;</i> <i>VI - quando a transferência for necessária para execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do art. 24; ou</i>

⁶ http://www.dof.gob.mx/nota_detalle.php?codigo=5346597&fecha=29/05/2014.

Tema	PL 5276/2016	Visão ABRANET
		<p><i>VII - quando o titular tiver fornecido o seu consentimento para a transferência, com informação prévia a específica sobre o caráter internacional da operação, com alerta quanto aos riscos envolvidos.</i></p> <p><i>VIII - quando o responsável pelo tratamento comprovar que a transferência se baseia em cláusulas contratuais padrão aprovadas pelo órgão competente ou em regras e códigos internacionalmente aceitos;</i></p> <p><i>IX - quando o responsável pelo tratamento comprovar que detém selos, certificados ou códigos de conduta e adequação emitidos por organismos de certificação qualificados e aprovados pelo órgão competente.</i></p> <p><i>Parágrafo único. O nível de proteção de dados do país estrangeiro será avaliado pelo órgão competente, que levará em conta:</i></p> <p><i>I - as normas gerais e setoriais da legislação em vigor no país de destino;</i></p> <p><i>II - a natureza dos dados;</i></p> <p><i>III - a observância dos princípios gerais de proteção de dados pessoais previstos nesta Lei;</i></p> <p><i>IV - a adoção de medidas de segurança previstas em regulamento;</i></p> <p><i>V - as outras circunstâncias específicas relativas à transferência.</i></p> <p><i>Art. 34. A autorização referida no inciso IV do caput do art. 33 será concedida quando o responsável pelo tratamento apresentar garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular e será dispensável nas hipóteses dos incisos VIII e IX do art. 33 desta Lei.</i> <i>apresentadas em cláusulas contratuais aprovadas pelo órgão competente para uma transferência específica, em cláusulas contratuais padrão ou em normas corporativas globais, nos termos do regulamento.</i></p> <p><i>§1º O órgão competente poderá elaborar cláusulas contratuais padrão ou homologar dispositivos constantes em documentos que fundamentem a transferência internacional de dados, que deverão observar os princípios gerais de proteção de dados e os direitos do titular, garantida a responsabilidade solidária do cedente e do cessionário, independentemente de culpa.</i></p> <p><i>§2º Os responsáveis pelo tratamento que fizerem parte de um mesmo grupo econômico ou conglomerado multinacional poderão submeter normas corporativas globais à aprovação do órgão competente, obrigatórias para todas as empresas integrantes do grupo ou do conglomerado, a fim de obter permissão para transferências internacionais de dados dentro</i></p>

Tema	PL 5276/2016	Visão ABRANET
		<p><i>do grupo ou do conglomerado sem necessidade de autorizações específicas, observados os princípios gerais de proteção e os direitos do titular.</i></p> <p><i>§3º Na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação do órgão competente, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento.</i></p> <p><i>§4º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no caput serão, também, analisadas de acordo com o previsto nos §1º e §2º do art. 45”.</i></p>
<p>7. Autoridade competente</p>	<p><i>Art. 53. O órgão competente designado para zelar pela implementação e pela fiscalização desta Lei terá as seguintes atribuições:</i></p> <p><i>I- Zelar pela proteção dos dados pessoais, nos termos da legislação;</i></p> <p><i>II- Elaborar diretrizes para um Política Nacional de Proteção de Dados Pessoais e Privacidade;</i></p> <p><i>III- Realizar auditoria nos tratamentos de dados pessoais e processos envolvidos com dados pessoais visando garantir a sua conformidade aos princípios e regras desta Lei;</i></p> <p><i>IV- Promover entre a população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e as medidas de segurança;</i></p> <p><i>V- Promover estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;</i></p>	<p>Comentário:</p> <p>Se a opção do legislador for pela existência de autoridade, a ABRANET ressalta que deve existir uma estrutura autônoma, que seja neutra e equidistante para avaliar todos objetivos desenvolvimentistas de nosso país envolvidos, desde a proteção dos dados dos usuários até o progresso tecnológico e a livre iniciativa, com independência e orçamento próprio, desvinculado de eventuais sanções pecuniárias que venham a ser aplicadas pela entidade e que de acordo com os princípios do Estado Democrático de Direito tenha a sua atuação restrita pela expressão "<i>de acordo com os limites e princípios previstos na presente lei</i>". Em suma, a ABRANET sugere que a estruturação de uma eventual autoridade seja pautada pelos seguintes aspectos:</p> <ul style="list-style-type: none"> (i) membros escolhidos com base em múltiplas visões das questões de privacidade, com formação técnica prevalecendo sobre a política; (ii) capacidade de análise holística da proteção de dados, levando em conta os impactos na inovação, na economia, nas relações empresariais, internacionais e de consumo, e nas questões concorrenciais; e (iii) autonomia e orçamento próprio, desvinculado de eventuais sanções pecuniárias que venham a ser aplicadas pela entidade. (iv) limitação de discricionariedade e sistema de freios e contrapesos, notadamente para evitar impactos em sigilo e governança.

Tema	PL 5276/2016	Visão ABRANET
	<p><i>VI- Estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais.</i></p> <p><i>VII- Promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transacional;</i></p> <p><i>VIII- Dispor sobre as formas pelas quais se dará a publicidade das operações de tratamento;</i></p> <p><i>IX- Solicitar, a qualquer momento, às entidades do Poder Público que realizem operações de tratamento de dados pessoais, informe específico sobre o âmbito, natureza dos dados e demais detalhes de tratamento realizado, podendo emitir parecer técnico complementar para garantir o cumprimento desta Lei;</i></p> <p><i>X- Estabelecer normas complementares para as atividades de comunicação de dados pessoais;</i></p> <p><i>XI- Elaborar relatórios anuais acerca de suas atividades;</i></p> <p><i>XII- Editar normas sobre proteção de dados pessoais e privacidade; e</i></p> <p><i>XIII- Realizar demais ações dentro de sua esfera de competência, inclusive as previstas nesta Lei e em legislação específica.</i></p> <p><i>Art. 54. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto por quinze representantes titulares, e seus respectivos suplentes, dos seguintes órgãos:</i></p>	<p>Ademais, tendo em vista a pluralidade de interesses envolvidos no tratamento de dados, seria interessante considerar a hipótese de criação de um conselho consultivo multisetorial, como instância de apoio às decisões da referida autoridade de proteção de dados, enriquecendo-as com a contribuição dos mais distintos setores interessados.</p>

Tema	PL 5276/2016	Visão ABRANET
	<p>I- Sete representantes do Poder Executivo federal</p> <p>II- Um representante indicado pelo Congresso Nacional;</p> <p>III- Um representante indicado pelo Conselho Nacional de Justiça;</p> <p>IV- Um representante indicado pelo Conselho Nacional do Ministério Público;</p> <p>V- Um representante indicado pelo Comitê Gestor da Internet do Brasil;</p> <p>VI- Um representante da sociedade civil;</p> <p>VII- Um representante da academia; e</p> <p>VIII- Dois representantes do setor privado</p> <p>§ 1º Os representantes serão designados por ato do Ministro de Estado da Justiça e terão mandato de dois anos, permitida uma recondução.</p> <p>§ 2º A participação no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será considerada atividade de relevante interesse público, não remunerada.</p> <p>§3º Os representantes referidos no inciso I a V do caput e seus respectivos suplentes serão indicados pelos titulares dos respectivos órgãos e entidades.</p> <p>§ 4º Os representantes referidos nos incisos VI e VIII do caput e seus respectivos suplentes serão indicados na forma de regulamento.</p>	

Tema	PL 5276/2016	Visão ABRANET
<p>8. <i>Vacatio legis</i></p>	<p><i>Art. 56. Esta Lei entrará em vigor cento e oitenta dias após a data da sua publicação.</i></p>	<p><u>Comentário:</u></p> <p>A ABRANET entende que as mudanças propostas PL impactam profundamente o dia-a-dia da população brasileira e, principalmente, das empresas que atuam no Brasil. Assim, é preciso garantir uma vacatio legis proporcional para que a sociedade tenha tempo de assimilar todas as alterações promovidas pelo novo marco legal. Nesse sentido a sugestão abaixo:</p> <p><u>Sugestão</u></p> <p><i>Art. 56. Esta Lei entrará em vigor no prazo de 3 (três) anos contados da data da sua publicação.</i></p>