São Paulo, 5 de julho de 2015.

Ao
Ministério da Justiça
Secretaria Nacional do Consumidor – Senacon
At.: Exma. Secretaria Juliana Pereira da Silva

ABRANET – Associação Brasileira de Internet, fundada em 1996 com objetivo de congregar os provedores de Internet e atuar em defesa da Internet, saúda a iniciativa deste Ministério da Justiça de promover debate público sobre o Anteprojeto de Lei de Proteção de Dados Pessoais (APL).

A presente contribuição aponta as preocupações da Abranet em relação à minuta do APL em processo de consulta pública, bem como as principais sugestões e comentários que se encontram de forma mais sistemática no quadro anexo, além de também inseridas na plataforma do debate público.

I. Observações preliminares:

1. A Abranet apresenta suas observações tomando por base o texto da minuta submetida à consulta pública que, de maneira clara, inspira-se no modelo legislativo europeu de proteção de dados. A Associação, portanto, tomou essa opção do Ministério da Justiça como premissa e não discutiu a conveniência da aplicação desse modelo ao Brasil. Portanto, a presente manifestação não significa nem o apoio da Abranet à adoção do modelo europeu no Brasil, nem a discordância com tal opção.

2. No que diz respeito à jurisdição, a proposta do APL é que o âmbito de aplicação da lei estenda-se a pessoas jurídicas, independentemente do território de sua sede ou de localização do banco de dados, desde que a operação de tratamento ocorra no território nacional ou os dados pessoais em tratamento tenham sido coletados em território nacional. Para evitar conflitos de lei que venham a inibir investimentos em infraestrutura no país, ou mesmo oferta de serviços ao usuário brasileiro, a Abranet propõe que o conflito de leis não exclua a aplicação da lei estrangeira, quando esta apresentar nível de proteção equivalente para o Brasil.

3. Outro aspecto do APL que mereceu diversas sugestões e comentários da Abranet foi a discrepância existente na aplicação de hipóteses de exceção ao consentimento do titular de dados aplicáveis a entidades privadas e entidades públicas. O entendimento da associação 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.

II. Autoridade competente:

4. O texto do Anteprojeto de Lei apresenta, em diversas oportunidades, referência à autoridade competente, estabelecendo poderes regulamentares amplos a ela. No entanto, não há no texto qualquer balizamento que indique quem será essa autoridade, qual será sua composição e seu regime jurídico.

5. Tendo em vista a opção do Ministério da Justiça pelo modelo legislativo europeu, a Abranet entende que, dentro desse contexto, é importante que a proposta estabeleça uma autoridade com uma estrutura autônoma, que seja neutra e equidistante para avaliar todos os objetivos desenvolvimentistas envolvidos, desde a proteção de dados dos usuários até o progresso tecnológico e a livre iniciativa. Nesse sentido, a Abranet sugere que a estruturação de uma autoridade paute-se 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.
   (iii) Autonomia e orçamento próprio, desvinculado de eventuais sanções pecuniárias que venham a ser aplicadas pela entidade.

6. Em que pese a importância do estabelecimento de uma autoridade autônoma, técnica e única para coordenar e interpretar a lei que rege o tratamento de dados pessoais, algumas observações, comentários e sugestões da Abranet buscam melhor delimitar o alcance e o poder discricionário da "autoridade competente" a que se refere o texto do APL.

III. Definições:

7. Dentre as sugestões que a Abranet apresenta em relação às definições do texto do APL, especificamente em seu Artigo 5º, destacam-se as seguintes:

(i) Dado pessoal: a sugestão de redação é para definir mais claramente que os dados devem se referir à capacidade de identificação especificamente do indivíduo, considerados os meios razoavelmente utilizados;

(ii) Tratamento: a Abranet sugere a supressão de algumas ações do conceito de tratamento, por razões diversas, incluindo aspectos tributários e possível confusão com termos já definidos em outras normas legais;

(iii) Dados anônimos: não há uma sugestão alternativa de redação, mas uma observação de que o APL só traz o termo nas definições. É importante que o APL reconheça que o dado anônimo, exatamente por sua incapacidade de identificação individual, não é um dado pessoal, exceto se tratado para adquirir essa condição;

(iv) Consentimento: o entendimento da Abranet é de que o titular de dados tem a capacidade de consentir o tratamento de seus dados pessoais de diversas maneiras. A obrigatoriedade de que seja expresso não deve ser aplicada a todas as circunstâncias, mas apenas àquelas em que isso seja necessário para garantir que tenha ocorrido de maneira inequívoca;

(v) Dissociação e Reidentificação: a sugestão à definição de "dissociação" tem em vista a redação que a Abranet propôs para "dado pessoal";

(vi) Unificação de termos: a sugestão de unificar termos como "comunicação", "interconexão", "difusão" e "transferência" tem por objetivo simplificar a linguagem do APL, para tratar de uma única maneira as hipóteses em que o responsável pelo tratamento transfere e informa dados pessoais.

IV. Princípios:

8. A Abranet reconhece os princípios relacionados no APL como universalmente aceitos em matéria de proteção de dados pessoais. 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".

9. Dentre os princípios, a Abranet entende que é de grande importância o reconhecimento de que o tratamento de dados pessoais é benéfico, quando realizado em conformidade com os demais princípios, sendo parte integrante do processo de inovação e evolução da sociedade. Por isso, o princípio da livre iniciativa poderia ser adicionado ao respectivo capítulo, como forma de permitir desenvolvimento de novas aplicações do tratamento de dados pessoais, em conformidade com a lei.

V. Consentimento e suas exceções:

10. Conforme já mencionado no item correspondente a definições, a Abranet entende 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.

11. Dentro do espírito da legislação europeia, a sugestão da Abranet como regra geral de consentimento é de que, quando necessário, ele tenha que ser inequívoco, ou seja, perceptível pelo responsável pelo tratamento de dados pessoais, independente da forma que tenha ocorrido. O consentimento expresso ficaria, então, adstrito a casos específicos, como o tratamento de dados sensíveis.

12. Além disso, 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 relacionadas ao acesso a dados armazenados e a observância dos princípios estabelecidos na lei, com destaque à adequação e à finalidade, 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 na prestação de serviços e oferecimentos de produtos que são do interesse do próprio titular.

13. Ao exigir o consentimento da forma como faz o APL, 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. Uma forma de se gerar um ambiente no qual o consentimento não passa a ser exigido para todo e qualquer passo do tratamento de dados seria a inserção de um item no artigo 11, dentre as hipóteses em que o consentimento é dispensado, para contemplar as situações nas quais existe um “interesse legítimo” para que o tratamento ocorra.

14. Quanto ao Parágrafo 1º do Artigo 7º, que veda o consentimento do tratamento de dados como condição para o fornecimento de produto ou serviço, o entendimento da Abranet é de que tal dispositivo contraria a realidade, notadamente de serviços online que já integram a vida dos cidadãos.

15. No atual estágio de desenvolvimento da sociedade da informação diversos produtos e serviços, tais como aplicações que prescindem do acesso à internet somente têm possibilidade de atingir a funcionalidade permitida, mediante o fornecimento de dados inerente ao usuário que pretende fazer o uso de tal aplicação. Logo, a lei não pode ser avessa a uma realidade tão flagrante e em plena expansão.

16. Desta feita, a lei precisa ponderar tal condicionante tutelando tais situações mediante a aplicação do princípio da transparência, sendo assim facultado ao usuário ter a oportunidade de previamente ao uso de qualquer produto ou serviço, conhecer as informações que serão necessárias a tal utilização, e decidir de forma plena e convicta.

17. Um exemplo de serviços baseados em aplicações cuja funcionalidade não pode prescindir do consentimento para tratamento de dados pessoais são as aplicações que favorecem ou trazem alternativas à mobilidade urbana, como "apps" de serviços de taxi ou de serviços de navegação de trânsito por mapas, que permitem a identificação de melhores rotas para o deslocamento urbano. Tais ferramentas dependem da geolocalização do usuário e, em alguns casos, da identificação do número telefônico.

18. As sugestões e comentários apresentados em outros parágrafos do Artigo 7º têm o mesmo objetivo de contextualizar as diferentes formas de consentimento no universo do "Big Data" e da "Internet das Coisas", destacando que os excessos resultam, muitas vezes, na chamada fadiga do consentimento, tornando o ato menos consciente e, portanto, pouco eficaz.

19. No que se refere às hipóteses de dispensa do consentimento, a Abranet notou que, em que pese a inspiração europeia do APL, não há em seu texto um dispositivo equivalente à dispensa baseada no legítimo interesse do responsável pelo tratamento.

20. O reconhecimento do legítimo interesse do responsável para a dispensa do consentimento é uma importante disposição para garantir a inovação, em linha com os princípios estabelecidos no APL, e ainda preservar o direito de escolha do mesmo, permitindo assim experiências proveitosas, cômodas e fluídas de diversos serviços, o que se tornaria inviável com a mera obrigatoriedade de consentimento expresso.

21. A definição do legítimo interesse deve ser aberta e flexível, em vista da constante transformação da tecnologia e do próprio conceito de inovação. Embora a Europa venha discutindo se deve ou não haver um critério específico para o legítimo interesse, sempre tem sido reconhecida a sua importância, razão pela qual nunca se cogitou a sua supressão.

22. 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.

23. Ao atender aos critérios acima, o responsável pode enquadrar o tratamento como em legítimo interesse, sem a necessidade de quaisquer outras formalidades ou documentações.

VI. Dados anônimos:

24. Ainda no Artigo 11, uma importante sugestão é a inclusão de um parágrafo para esclarecer que o tratamento de dados anônimos, incluindo os dados pessoais que tenham passado por processo de dissociação, independe de consentimento, posto que, uma vez anonimizados, deixam de ter a característica de identificação individual que é inerente ao dado pessoal.

25. Ciente da justa preocupação com a possibildiade de cruzamento de dados anônimos ou dissociados, de maneira que passem a ter condição de identificação de seu titular, a Abranet sugere a inclusão da definição de dado reidentificado. Nesse caso, o dado anônimo ou dissociado que, por meio razoáveis volte a ter a condição de identificação individual, será considerado dado reidentificado e, por isso, volta a ser tratado como dado pessoal.

VII. Dados sensíveis:

26. Conforme mencionado acima, a regra geral do consentimento não deve estabelecer forma específica para seu reconhecimento, sob pena de fadiga e perda da sua eficácia. O tratamento de dados sensíveis, em razão de sua natureza, justifica que o titular dos dados tenha que consenti-lo de maneira expressa. Por essa razão, a Abranet sugere que o consentimento previsto no inciso I do Artigo 12 seja “expresso” ao invés de “especial”.

27. Em relação ao Parágrafo 2º do Artigo 12, a Abranet ressalta que algumas atividades, sobretudo relacionadas a análise de riscos (seguros, crédito e outros) depende da utilização de dados pessoais para a definição do perfil do cliente. Nesse caso, a proibição de uso de dados pessoais em detrimento do titular deve ser relativizada, para que o benefício da coletividade com a correta aferição de riscos prevaleça.

VIII. Término do Tratamento:

28. As sugestões da Abranet no capítulo referente ao término do tratamento de dados reflete o entendimento de que, uma vez que o titular dos dados exerça seu direito à autodeterminação e consinta o tratamento de dados, não há justificativa para que o Estado interfira nessa relação, estabelecendo prazos máximos.

29. A Abranet entende, também, que o Parágrafo único do Artigo 15, ao estabelecer a possibilidade de órgão competente determinar hipóteses específicas de conservação de dados pessoais ao responsável pelo tratamento, o APL cria um ônus injustificado. Caso o Estado tenha interesse na conservação de dados pessoais, deveria obter pelas vias legais o acesso a eles e então, cuidar de sua conservação.

IX. Direitos do titular:

30. Sobretudo no Artigo 17, a Abranet manifesta preocupação com a redação apresentada, uma vez que considera a possibilidade que alguns dispositivos venham a ser utilizados para afrontar direitos fundamentais do cidadão, como a liberdade de expressão e o acesso à informação.

31. Com efeito, 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. Neste mesmo sentido, 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, portanto.

32. A associação também sugere a adoção de critérios abertos para a definição dos prazos previstos para cumprimento, pelo responsável, de obrigações de fornecer informações, atualizar ou terminar o tratamento de dados. Enquanto o estabelecimento de cumprimento imediato é inviável em muitos casos, que dependem de ações tomadas ao longo de uma cadeia de atividades, a definição de prazos específicos parece inadequada, já que o mesmo prazo pode demonstrar-se excessivo em alguns casos e insuficiente em outros, de acordo com as circunstâncias específicas.

33. Da mesma forma, a Abranet entende que é irrazoável estabelecer formas específicas de fornecimento de informações pelo responsável pelo tratamento, de acordo com a vontade do titular dos dados ou seguindo formatos pré-estabelecidos por autoridades. Isso porque cada serviço ou atividade tem peculiaridades específicas. A lei deve

garantir que as informações requeridas sejam completas e inteligíveis, sem engessar a forma de apresentação.

34. Outra importante sugestão diz respeito à redação do Artigo 19, que estabelece a obrigação do responsável pelo tratamento de dados pessoais de informar critérios e procedimentos relacionados a decisões tomadas com base em tratamento automatizado de dados pessoais. A forma prevista no APL dá margem a violação de direitos de responsáveis, sobretudo no que diz respeito à proteção de segredos de negócios. É importante frisar que o sigilo de critérios, em muitos casos, é o que garante o efeito positivo do tratamento de dados para toda a sociedade, como casos em que o objetivo é redução de fraudes em operações financeiras.

X. Comunicação, interconexão e transferência de dados:

35. Conforme mencionado anteriormente, a Abranet sugere o ajuste das definições, para que qualquer transferência de dados pessoais seja colocada sob uma mesma nomenclatura. Nesse sentido, “comunicação”, “interconexão” devem incorporar a definição de “transferência”. Além disso, o termo “interconexão” é tipicamente utilizado em normas de telecomunicações, em sentido diverso e bastante específico, o que poderia causar confusão.

36. O estabelecimento de responsabilidade solidária entre cedente e cessionário não é uma norma razoável, uma vez que as obrigações de um e outro não são, necessariamente, as mesmas, dependendo da natureza da relação entre eles ou mesmo entre eles e o titular dos dados. Vale observar que o titular dos dados pode ter consentido com a comunicação de seus dados ao cessionário com finalidade distinta daquela esperada do cedente.

37. Outro dispositivo que despertou preocupação da Abranet foi o Artigo 27, que prevê a possibilidade de órgão competente estabelecer normas complementares para as atividades de comunicação e interconexão de dados pessoais. Preliminarmente, a Abranet faz referência aos seus comentários ao artigo 1º , onde procurou esclarecer que as informações fornecidas nesta lei sobre a atuação de uma “autoridade” são escassas e não permitem a plena contribuição e, ao mesmo tempo, deixar claro o que entende como premissas mínimas para existência de autoridade.

38. Mesmo diante dessas incertezas, um aspecto é indissociável do Estado Democrático de Direito: a atuação da autoridade competente deve restringir-se pela expressão "de acordo com os limites e princípios previstos na presente lei". O poder discricionário

dado à autoridade competente neste artigo poderia fazer com que, sem o devido debate no Legislativo, uma autoridade crie novas normas limitadoras de atividades lícitas, o que é inadmissível em nosso Ordenamento.

39. De todo modo, a melhor análise do dispositivo de Lei dependerá seguramente da especificação das regras de criação da autoridade específica e independente para a proteção de dados no País. O desenho dessa autoridade oferecerá condições para que se verifique se está diante de uma oportunidade de favorecer, dentre outros fatores, a segurança jurídica e inovação em questões que vem pautando a agenda do País nos fóruns internacionais.

40. Tendo em vista a pluralidade de interesses envolvidos no tratamento de dados pessoais, seria interessante considerar a hipótese de criação de um conselho consultivo multisetorial, como instância de apoio às suas decisões, enriquecendo-as com a contribuição dos mais distintos setores interessados.

XI. Transferência Internacional de Dados:

41. O modelo adotado no APL, de adequação entre diferentes legislações tem se provado ineficiente e burocrático na Europa, tornando casuísticas as exceções em alguns casos. Em outros, o reconhecimento da adequação da legislação não leva em consideração se há medidas práticas que garantam sua aplicação. Ademais, em razão do funcionamento da internet e da infraestrutura de telecom no mundo, a comunicação de um dado pode extrapolar as fronteiras do país sem que o responsável ou o operador tenha poder ou gerência para restringir isso, ainda que o dado seja armazenado no Brasil.

42. Por esses motivos, 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, independente de onde os dados pessoais sejam tratados. O importante é a responsabilidade do responsável diante do titular.

43. A Abranet observa, ainda, que o Artigo 28, ao 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.

44. Além disso, a hipótese de transferência internacional mediante consentimento específico para essa finalidade, prevista no Artigo 29, pode ser incluída como inciso do

Artigo 28. No entanto, vale ressaltar que o inciso II do Artigo 29 deve ser excluído, já que a informação sobre riscos envolvidos e detalhamento de vulnerabilidades do país de destino resulta em dados subjetivos, que praticamente inviabilizariam a hipótese de transferência mediante consentimento, afrontando a vontade do próprio titular dos dados.

45. 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, independente dos outros critérios mencionados na lei. Além disso, conforme já mencionado anteriormente, a regra de solidariedade entre cedente e cessionário não parece razoável, uma vez que as obrigações perante o titular de dados pode ser distinta, 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 rspectivas perante o titular dos dados.

46. Finalmente, em vista do caráter internacional, a Abranet sugere que o ordenamento jurídico brasileiro reconheça regras já existentes e adotadas internacionalmente, já incorporadas ao sistema internacional de proteção de dados pessoais, na medida de sua compatibilidade com a lei brasileira.

XII. Responsabilidade dos Agentes:

47. O entendimento da Abranet é que a identificação e distinção entre o responsável e o operador são exatamente a diferenciação da atividade de cada um deles e, consequentemente, os atos pelos quais podem ser responsáveis. Por isso, o Artigo 35 e seguintes devem afastar regras de responsabilidade solidária e esclarecer qual é a de cada parte na cadeia de atividades.

48. Traz grande preocupação à Abranet a previsão do Artigo 40 e seu parágrafo único, que estabelece obrigação de manutenção de registro das operações de tratamento de dados pessoais e que órgão competente poderá dispor sobre formato, estrutura e tempo de guarda de registro.

49. Preliminarmente, a Abranet faz referência aos seus comentários ao artigo 1º , onde procurou esclarecer que as informações fornecidas nesta lei sobre a atuação de uma “autoridade” são escassas e não permitem a plena contribuição e, ao mesmo tempo, deixar claro o que entende como premissas mínimas para existência de autoridade.

50. Em segundo lugar, Abranet entende que a lei deveria limitar-se a disciplinar o comando relativo ao direito em questão, abstendo-se de regular os formatos para sua entrega. Isso, para não impedir o livre desenvolvimento das inovações e da própria

competição positiva ao consumidor que pode estimular o fornecedor a dar o melhor acesso como diferencial.

51. Cabe à lei disciplinar o direito e exigir seu cumprimento, devendo, no entender da Abranet, abster-se de regular as formas, sob pena de engessamento e superregulação do tema, de todo prejudiciais ao mercado em geral.

XIII. Segurança e sigilo de dados:

52. O entendimento da Abranet é que o Artigo 44, que estabelece a obrigação de comunicação imediata de um incidente de segurança que possa causar prejuízo aos titulares, deve ser revisto. Isso porque um incidente de segurança somente pode identificar a extensão de danos e de riscos envolvidos após uma cuidadosa investigação interna. Apenas após essa análise é possível saber se há potencial de risco.

53. A outra preocupação da Abranet nesse capítulo é a previsão do Artgo 47, que dá ao órgão competente o poder de estabelecer normas complementares, acerca de critérios e padrões mínimos de segurança. Tal perocupação decorre da inconveniência de tratar em textos legais quaisquer padrões técnicos e tecnológicos, em vista da sua rápida obsolescência.

54. A mesma preocupação com definição de tecnologia aplica-se ao Artigo 49, segundo o qual o órgão competente estimulará a adoção de certos softwares e padrões técnicos que facilitem a disposicão de titulares sobre seus dados pessoais. Tal proposta, além de ficar longe de definir a quais parâmetros e critérios se refere, tende a tornar-se barreira ao desenvolvimento tecnológico e à inovação, em vista da rápida evolução da tecnologia ou mesmo de interferir na livre iniciativa privada.

XIV. Sanções Administrativas:

55. A Abranet entende ser importante destacar no capítulo correspondente a sanções administrativas os princípios da razoabilidade e da proporcionalidade, bem como a definição de critérios mais específicos para a aplicação de multa, com a definição de um valor máximo.

56. É importante, ainda, que eventuais sanções considerem também circunstâncias específicas em favor do responsável pelo tratamento de dados pessoais, como a existência de programas internos de privacidade, a velocidade de introdução e adoção de fatores de correção e a ausência de dolo ou mesmo do impacto de determinadas

penalidades que podem acarretar o efetivo encerramento da atividade de determinada empresa no país.

XV. Vigência:

57. O prazo de 120 (cento e vinte dias) contados da data de publicação para a entrada em vigência da lei é certamente insuficiente para a implementação de todas as medidas necessárias para seu cumprimento por parte dos responsáveis pelo tratamento de dados pessoais. O prazo de dois anos deve ser considerado ou, no mínimo, de um ano.

QUADRO ANEXO

Anteprojeto de Lei para a Proteção de Dados Pessoais	Comentário e Sugestões
Anteprojeto de Lei	
Dispõe sobre o tratamento de dados pessoais para proteger a personalidade e a dignidade da pessoa natural	**Comentário:** O projeto de lei faz referência a uma "autoridade competente" para regular o tratamento de dados pessoais, no entanto, não prevê a criação de um órgão independente em seu preâmbulo. Ao mesmo tempo em que muitas disposições ao longo desta proposta conferem poderes discricionários amplos para essa "autoridade", não se observa o devido balizamento na própria lei, o que limita as possibilidades de comentário às disposições. Se a opção do legislador for pela existência de autoridade, 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.
A **PRESIDENTA DA REPÚBLICA** Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei	
CAPÍTULO I – DISPOSIÇÕES PRELIMINARES	
Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, com o objetivo de proteger os direitos fundamentais de liberdade, intimidade e privacidade da pessoa natural.	**Comentário**: A redação atual utiliza os termos "intimidade e privacidade da pessoa natural", o que destoa da redação do art. 5º, X, da CF, que usa as expressões "intimidade e vida privada". À luz do que já faz o Marco Civil da Internet, seria interessante uniformizar a linguagem em volta do termo "privacidade", já que o mesmo conecta o debate nacional com a linguagem internacional sobre o tema, reduz confusões terminológicas, além de favorecer a discussão abaixo mencionada sobre o papel das pessoas jurídicas no regime de tutela dos dados pessoais; **Sugestão**: § 1º A disciplina da proteção de dados no Brasil tem como

	fundamento o respeito à privacidade, bem como: I – liberdade de expressão e opinião; III- a livre iniciativa, a livre concorrência e a defesa do consumidor; e II- o desenvolvimento tecnológico do país. **Comentário:** É imprescindível que o estabelecimento de um marco legal sobre privacidade considere não apenas os aspectos diretamente ligados à defesa imediata do consumidor, mas, também e talvez principalmente, o bem-estar que lhe é gerado através da livre iniciativa e concorrência, sua defesa mediata, e que geram inovação e um ciclo virtuoso de incremento qualitativo dos produtos por meio da competição. Também seria impensável um marco legal que desconsiderasse a liberdade de expressão e opinião e que atravancasse tais atividades. Como não existem direitos absolutos, é imprescindível que esta lei considere tais princípios, a exemplo do recentíssimo Marco Civil da Internet. **Sugestão**: § 2º "Os princípios expressos nesta Lei não excluem outros previstos no sistema legislativo brasileiro, relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja signatária".
Art. 2º Esta Lei aplica-se a qualquer operação de tratamento realizada por meio total ou parcialmente automatizado, por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do país de sua sede e do país onde esteja localizado o banco de dados, desde que:	**Sugestão /Comentário**: Considerando a previsão deste artigo para que a lei seja aplicável a qualquer indivíduo ou pessoa jurídica, ainda que estrangeiros, sugerimos incialmente a inclusão do seguinte parágrafo: "Em caso de conflito entre leis, a aplicação da presente lei não excluirá a aplicação de legislação estrangeira, desde que este país possua nível equivalente de proteção para o Brasil”.
I – a operação de tratamento seja realizada no território nacional; ou	

II – os dados pessoais objeto do tratamento tenham sido coletados no território nacional.	
§1º - Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.	
§ 2º - Esta Lei não se aplica aos tratamentos de dados:	**Sugestão**: Sugerimos a adição de outro parágrafo com a seguinte redação: **"**A aplicação desta Lei não excluirá ou afastará a lei estrangeira de países que proporcionem nível de proteção de dados pessoais equiparável ao desta Lei nas hipóteses de conexão ou conflito de leis no âmbito internacional"
I – realizados por pessoa natural para fins exclusivamente pessoais; ou	**Sugestão:** I – realizados por pessoa natural, dentro de um contexto privado, para fins exclusivamente pessoais.
II – realizados para fins exclusivamente jornalísticos.	Sugestão: III – quando o tratamento se restringir a dados anônimos.
§ 3º - É vedado aos órgãos públicos e entidades públicas efetuar a transferência de dados pessoais constantes de bases de dados que administram ou a que tenham acesso no exercício de suas competências legais para entidades privadas, exceto em casos de execução terceirizada ou mediante concessão e permissão de atividade pública que o exija e exclusivamente para fim específico e determinado.	**Comentário:** A transferência deve se dar no limite da finalidade do órgão ou entidade.
Art. 3º - As empresas públicas e sociedades de economia mista que atuem em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.	
Parágrafo único. As empresas públicas e 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 entidades públicas, nos termos dessa Lei.	
Art. 4º Os tratamentos de dados pessoais para fins exclusivos de segurança pública, defesa, segurança do Estado, ou atividades de investigação e repressão de infrações penais, serão regidos por legislação específica,	

observados os princípios gerais de proteção e os direitos do titular previstos nesta Lei.	
Parágrafo único. É vedado o tratamento dos dados a que se refere o caput por pessoa de direito privado, salvo em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico ao órgão competente.	
Art. 5º Para os fins desta Lei, considera-se:	**Sugestão/Comentário:** Definir o que seriam "dados públicos de acesso irrestrito". O APL, em seu art. 11, §1º, exclui a exigência de consentimento para o tratamento de "dados públicos de acesso irrestrito". A exceção poderia ser questionada dada a ampla abrangência do termo invocado, especialmente quando se leva em consideração que o APL não define o que são tais "dados públicos de acesso irrestrito".
I – dado pessoal: dado relacionado à pessoa natural identificada ou identificável, inclusive a partir de números identificativos, dados locacionais ou identificadores eletrônicos;	**Sugestão: I –** dado pessoal: dado relacionado à pessoa natural identificada ou identificável no nível individual, inclusive a partir de números identificativos, dados locacionais ou identificadores eletrônicos, desde que tais permitam a identificação, através de formas razoáveis, da pessoa natural pelo responsável pelo tratamento de dados pessoais;
II – tratamento: conjunto de ações referentes a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, transporte, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, bloqueio ou fornecimento a terceiros de dados pessoais, por comunicação, interconexão, transferência, difusão ou extração;	**Comentário**: Algumas das ações incluídas nessa definição podem trazer resultados adversos: - A mera recepção não deve ser considerada como tratamento de dados, já que só configuraria efetiva capacidade de uso dos dados na medida em que executar outra ação de tratamento (armazenamento, processamento, etc.). - Transporte não deve ser incluído, uma vez que tem o mesmo significado de transmissão neste contexto, sem contar que poderia abranger, indevidamente, transporte físico. Finalmente, há risco tributário na inclusão da atividade de transporte. - Interconexão é um termo que pode, tranquilamente, ser abrangido pela

	definição de transmissão. Além disso, é tipicamente utilizado com outras características em telecomunicações e também pode trazer consequências tributárias (incide ICMS sobre interconexão em telecomunicações)**.**
III – dados sensíveis: dados pessoais que revelem a origem racial ou étnica, as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, bem como dados genéticos;	
IV – dados anônimos: dados relativos a um titular que não possa ser identificado, nem pelo responsável pelo tratamento nem por qualquer outra pessoa, tendo em conta o conjunto de meios suscetíveis de serem razoavelmente utilizados para identificar o referido titular;	**Sugestão: IV** – 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.
V – banco de dados: conjunto estruturado de dados pessoais, localizado em um ou em vários locais, em suporte eletrônico ou físico;	
VI – titular: a pessoa natural a quem se referem os dados pessoais objeto de tratamento;	
VII – consentimento: manifestação livre, expressa, específica e informada pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;	**Comentário:** A definição do consentimento é uma das partes mais controversas do projeto. Em algumas discussões a palavra “expressa” vem sendo apontada como uma preocupação pelas empresas de internet, por possibilitar a interpretação de que a cada novo uso ou coleta de dados um novo consentimento deveria ser fornecido, o que pioraria muito, ou quase inviabilizaria, a experiência do usuário na internet. Ao invés de alterar ou remover a palavra “expressa” o projeto traz ainda a previsão do consentimento também “específico”, reforçando a ideia de diferentes consentimentos para diferentes usos. Dessa forma, recomenda-se a seguinte alteração:

	Sugestão: VII – consentimento: Toda manifestação inequívoca realizada pelo titular de dados de maneira livre e informada, na qual autorize o tratamento de seus dados pessoais.
VIII – responsável: a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;	
IX – operador: a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do responsável;	
X – comunicação de dados: transferência de dados pessoais a um ou mais sujeitos determinados diversos do seu titular, sob qualquer forma;	**Sugestão/Comentário:** Sugerimos a fusão dos termos "comunicação de dados", "interconexão", "difusão" e "transferência", preferencialmente ampliando a definição de "transferência" para abranger todas as definições.
XI – interconexão: transferência de dados pessoais de um banco a outro, mantido ou não pelo mesmo proprietário, com finalidade semelhante ou distinta;	**Sugestão /Comentário:** Sugerimos a fusão dos termos "comunicação de dados", "interconexão", "difusão" e "transferência", preferencialmente ampliando a definição de "transferência" para abranger todas as definições. Além disso, a palavra "interconexão" tem outro significado em normas de telecomunicações e pode trazer impactos tributários.
XII – difusão: transferência de dados pessoais a um ou mais sujeitos indeterminados, diversos do seu titular, sob qualquer forma;	**Sugestão /Comentário:** Sugerimos a fusão dos termos "comunicação de dados", "interconexão", "difusão" e "transferência", preferencialmente ampliando a definição de "transferência" para abranger todas as definições.
XIII – transferência internacional de dados: transferência de dados pessoais para um país estrangeiro;	**Sugestão /Comentário:** Sugerimos a fusão dos termos "comunicação de dados", "interconexão", "difusão" e "transferência", preferencialmente ampliando a definição de "transferência" para abranger todas as definições.
XIV – dissociação: ato de modificar o dado pessoal de modo a que ele não possa ser associado, direta ou indiretamente, com um indivíduo identificado ou identificável;	**Sugestão: XIV**- dissociação: Modificar o dado pessoal de modo que não possa identificar seu titular no nível individual, tornando-o um dado anônimo. **Comentário:** A definição de dissociação deve se referir expressamente à

	condição de anonimato dos dados dissociados. Essa mudança garantiria que dados dissociados deixariam de ter a interpretação essencial à continuidade da inteligência de Big Data. **Sugestão (nova definição):** Dado reidentificado: dado anônimo ou dado pessoal que tenha passado por processo de dissociação, quando o responsável o submete a tratamento que lhe confira a capacidade de identificação do seu titular, no nível individual. **Comentário:** A definição de "reidentificação" é importante para distinguir o dado que é efetivamente incapaz de identificação positiva daquele resultante do tratamento que o transforma em dado identificável.
XV – bloqueio: guarda do dado pessoal ou do banco de dados com a suspensão temporária de qualquer operação de tratamento;	
XVI – cancelamento: eliminação de dados ou conjunto de dados armazenados em banco de dados, seja qual for o procedimento empregado;	
XVII – uso compartilhado de dados: a comunicação, a difusão, a transferência internacional, a interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos, no cumprimento de suas competências legais, ou entre órgãos e entidades públicos e entes privados, com autorização específica, para uma ou mais modalidades de tratamento delegados por esses entes públicos; e	**Sugestão**: Padronizar a nomenclatura, como nas outras sessões. Sugerimos a fusão dos termos "comunicação de dados", "interconexão", "difusão" e "transferência", preferencialmente ampliando a definição de "transferência" para abranger todas as definições.
XVIII – encarregado: pessoa natural, indicada pelo responsável, que atua como canal de comunicação perante os titulares e o órgão competente.	
Art. 6º - As atividades de tratamento de dados pessoais deverão atender	**1. Sugestão/ Comentário**: Inserção de princípio que venha a prestigiar a

aos seguintes princípios gerais:	liberdade de iniciativa no tratamento de dados, desde que respeitada as condições impostas pela lei, como forma de fazer valer a menção a “direitos fundamentais de liberdade” previsto no artigo 1º.
I – princípio da finalidade, pelo qual o tratamento deve ser realizado com finalidades legítimas, específicas, explícitas e conhecidas pelo titular;	**Sugestão:** substituir “específicas, explícitas e conhecidas” por “devidamente informadas”. **Comentário:** Considerando a tecnologia de Big Data, a finalidade precisa ser inserida dentro de um contexto moderno. Muitas vezes o propósito surge durante o processamento de dados. Buscar propósitos específicos e literais ocasionaria a impossibilidade de operar mecanismos de buscas.
II – princípio da adequação, pelo qual o tratamento deve ser compatível com as finalidades almejadas e com as legítimas expectativas do titular, de acordo com o contexto do tratamento;	
III – princípio da necessidade, pelo qual o tratamento deve se limitar ao mínimo necessário para a realização das finalidades almejadas, abrangendo dados pertinentes, proporcionais e não excessivos;	**Sugestão/comentário:** Sugere-se substituir a palavra "mínimo" por "razoavelmente", para contemplar as situações em que o tratamento não é exigido, mas é recomendável ou útil para benefícios do usuário, como, por exemplo, em questões de segurança de sistemas ou para o fornecimento de serviços avançados ou compatíveis.
IV – princípio do livre acesso, pelo qual deve ser garantida consulta facilitada e gratuita pelos titulares sobre as modalidades de tratamento e sobre a integralidade dos seus dados pessoais;	**Sugestão/comentário:** Exclusão. Já está contido na transparência.
V – princípio da qualidade dos dados, pelo qual devem ser garantidas a exatidão, a clareza e a atualização dos dados, de acordo com a periodicidade necessária para o cumprimento da finalidade de seu tratamento;	**Comentário:** A redação desse artigo pode levar a interpretação de que o responsável tem obrigações pela correção da informação coletada. Os dados normalmente são coletados conforme disponibilizados, sendo irrazoável que seja obrigado a confirmar a veracidade zelar por sua atualização. O princípio deveria ser definido como aquele que garanta “a integridade dos

	dados coletados para cumprir os seus respectivos efeitos de tratamento legalmente autorizado". **Sugestão:** "Princípio da qualidade dos dados, pelo qual devem ser presumidas a exatidão, a clareza e a atualização dos dados informados pelo titular, admitindo-se prova em contrário e atualização de acordo com a periodicidade necessária para o cumprimento da finalidade de seu tratamento" Alternativamente, sugere-se a exclusão, uma vez que não cabe ao responsável zelar pela correção da informação coletada conforme disponibilizada pelo usuário.
VI – princípio da transparência, pelo qual devem ser garantidas aos titulares informações claras e adequadas sobre a realização do tratamento;	
VII – princípio da segurança, pelo qual devem ser utilizadas medidas técnicas e administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;	
VIII – princípio da prevenção, pelo qual devem ser adotadas medidas capazes de prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; e	
IX – princípio da não discriminação, pelo qual o tratamento não pode ser realizado para fins discriminatórios.	**Comentário:** O princípio da não-discriminação deve definir que "o tratamento não pode ser realizado para efeitos de discriminação ilícita". A razão é que a discriminação com base em dados pessoais é razoável em

	diversas atividades que exigem a definição de um perfil de cliente para analisar os riscos, tais como análise de crédito e de seguros. A lei não deve excluir a discriminação positiva.
§ 1º Os órgãos públicos darão publicidade às suas atividades de tratamento de dados por meio de informações claras, precisas e atualizadas em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos, respeitando o princípio da transparência disposto no inciso VI.	**Sugestão:** Completar com "e demais princípios estabelecidos nesta Lei".
§ 2º O uso compartilhado de dados pessoais deve atender a finalidade específica de execução de políticas públicas e atribuição legal pelos órgãos e entidades públicas, respeitando o princípio da finalidade, adequação e necessidade dispostos nos incisos I, II e III.	**Sugestão:** Completar com "e demais princípios estabelecidos nesta Lei".
CAPÍTULO II – REQUISITOS PARA O TRATAMENTO DE DADOS PESSOAIS	
Seção 1 – Consentimento	
Art. 7º O tratamento de dados pessoais somente é permitido após o consentimento livre, expresso, específico e informado do titular, salvo o disposto no art. 11.	**Sugestão/comentário:** O consentimento já está definido como livre, expresso, específico e informado no artigo 5º, VII. Fizemos a sugestão de alteração na definição. De qualquer modo, o Art. 7º, para evitar redundância, deve resumir-se a "O tratamento de dados pessoais somente é permitido após o consentimento do titular, salvo o disposto no art.11."
§1º O consentimento para o tratamento de dados pessoais não pode ser condição para o fornecimento de produto ou serviço ou para o exercício de direito, salvo em hipóteses em que os dados forem indispensáveis para a	**Sugestão:** Sugerimos a exclusão desse artigo. **Comentário:** O parágrafo 1º do artigo 7º parte de premissa equivocada ao prever que a recusa de consentimento não pode ser condição para o

sua realização.	fornecimento de produto ou serviço. No atual estágio de desenvolvimento da sociedade da informação diversos produtos e serviços, tais como aplicações que prescindem do acesso à internet somente têm possibilidade de atingir a funcionalidade permitida, mediante o fornecimento de dados inerente ao usuário que pretende fazer o uso de tal aplicação. Logo, a lei não pode ser avessa a uma realidade tão flagrante e em plena expansão. Desta feita, a lei precisa ponderar tal condicionante tutelando tais situações mediante a aplicação do princípio da transparência, sendo assim facultado ao usuário ter a oportunidade de previamente ao uso de qualquer produto ou serviço, conhecer as informações que serão necessárias a tal utilização, e decidir de forma plena e convicta. Alguns exemplos mais comuns que embasam nossas constatações: APP GPS: - Utilização de aplicativo com funcionalidade de GPS, comumente utilizado no trânsito: A não abertura de um dado como a geolocalização do usuário, inviabiliza a utilização da aplicação por este usuário em si. E em uma escala maior, funcionalidades como tempo de percurso e nível de congestionamento em determinadas vias deixariam de existir à medida em que outros usuários não concordem com o tratamento de seus dados. APP Taxi: - a utilização de aplicativos desta natureza também teriam seu modelo de negócio comprometido à medida em que a oposição à abertura de dados como o número de telefone do usuário e sua geolocalização inviabilizariam a funcionalidade do app. **Sugestão:** alternativamente, sugerimos a seguinte redação: **§1º** O consentimento para o tratamento de dados pessoais não pode ser condição para o fornecimento de produto ou serviço ou para o exercício de

	direito, **salvo quando tal fato decorrer da natureza própria do negócio jurídico ou** em hipóteses em que os dados forem indispensáveis para a sua realização.
§2º É vedado o tratamento de dados pessoais cujo consentimento tenha sido obtido mediante erro, dolo, estado de necessidade ou coação.	**Sugestão: § 2º:** É vedado o tratamento de dados pessoais cujo consentimento tenha sido obtido de forma ilícita. (sugestão em linha com o art.10, VII §1º). **Comentário:** "Erro" deve ser excluído desse rol. No caso de um erro de consentimento, todo o tratamento dos dados apresentados antes da comunicação do erro não deve ser considerado como indevido. A lei já garante o direito de revogação, caso o titular tenha incorrido em erro. Em relação ao dolo, estado de necessidade e coação, melhor seria tratar todas as hipóteses ilícitas de uma forma genérica.
§3º O consentimento deverá ser fornecido por escrito ou por outro meio que o certifique.	**Sugestão/ comentário:** A forma como o consentimento é fornecido, por escrito ou não, é irrelevante, principalmente atualmente. O § 8º do mesmo artigo já prevê que o responsável pelo tratamento dos dados tem o ônus da prova do consentimento. Portanto, a redação dos Parágrafos 3º e 8º deve ser fundida em um parágrafo só: "O consentimento deve ser fornecido por qualquer meio, nos termos da legislação vigente".
§4º O consentimento deverá ser fornecido de forma destacada das demais cláusulas contratuais.	**1. Sugestão/ comentário:** Essa exigência pode ser atendida por termos técnicos (criando-se uma caixa de seleção específica nos formulários de cadastro e etc.). Todavia, deve ser uma exigência apenas nos casos em que o consentimento expresso é necessário (p.ex dados sensíveis.)
§5º O consentimento deverá se referir a finalidades determinadas, sendo nulas as autorizações genéricas para o tratamento de dados pessoais.	**Sugestão/ comentário:** Como mencionado anteriormente, esse tipo de restrição afeta negativamente os mecanismos de pesquisa e de Big Data, o conceito de propósito compatível deve ser inserido e melhor trabalhado na legislação.
§6º O consentimento pode ser revogado a qualquer momento, sem ônus	**Comentário:** É importante assegurar que, apesar da revogação não ter

para o titular.	custos ao usuário, este pode estar sujeito a consequências como a perda da gratuidade de alguns serviços, a indisponibilidade de outros, ou mesmo ao cumprimento de obrigações que não se relacionam com o pedido de cancelamento. **Sugestão:** Neste sentido, será importante a remoção do § 1º deste artigo. Alternativamente, sugere-se a seguinte redação: **§6º** O consentimento pode ser revogado a qualquer momento, por procedimento gratuito.
§7º São nulas as disposições que estabeleçam ao titular obrigações iníquas, abusivas, que o coloquem em desvantagem exagerada, ou que sejam incompatíveis com a boa-fé ou a equidade.	**Sugestão:** Recomendamos a introdução de mais um Parágrafo com o disposto: § - Sem prejuízo do disposto nos parágrafos antecedentes, o consentimento se presume quando atendidos os seguintes requisitos: I - o titular agir de maneira inequívoca e compatível com a outorga do consentimento, respeitado o disposto no §2º deste Art. 7º; e II- os usos e costumes relativos ao negócio jurídico realizado entre titular e responsável forem compatíveis com o consentimento e a finalidade do negócio jurídico, observado o disposto no § 5º deste Art. 7º.
§8º Cabe ao responsável o ônus da prova de que o consentimento do titular foi obtido em conformidade com o disposto nesta Lei.	
Art. 8º O titular de dados pessoais com idade entre doze e dezoito anos idade poderá fornecer consentimento para tratamento que respeite sua condição peculiar de pessoa em desenvolvimento, ressalvada a possibilidade de revogação do consentimento pelos pais ou responsáveis legais, no seu melhor interesse.	
Art. 9º No caso do titular de dados pessoais com idade até doze anos incompletos, o consentimento será fornecido pelos pais ou responsáveis legais, devendo o tratamento respeitar sua condição peculiar de pessoa em desenvolvimento.	**Comentário:** Entendemos que a "respeitar condição peculiar" de menor de idade, como "pessoa em desenvolvimento", não deve ser um dever do responsável pelo tratamento de dados. Se o consentimento deve ser fornecido pelos pais, é deles a decisão de escolher qual o conteúdo

	adequado, como parte do controle dos pais. **Sugestão:** Sugerimos a remoção deste artigo ou a alteração do texto para: "No caso do titular de dados pessoais de até doze anos de idade, o consentimento deverá ser dado pelos pais ou responsáveis legais".
Art. 10º No momento do fornecimento do consentimento, o titular será informado de forma clara, adequada e ostensiva sobre os seguintes elementos:	
I – finalidade específica do tratamento;	**Sugestão/ comentário:** Conforme mencionado, finalidade específica pode ser incompatível com o atual uso de dados. Sugere-se a remoção de "específica".
II – forma e duração do tratamento;	
III – identificação do responsável;	
IV – informações de contato do responsável;	
V – sujeitos ou categorias de sujeitos para os quais os dados podem ser comunicados, bem como âmbito de difusão;	
VI – responsabilidades dos agentes que realizarão o tratamento; e	
VII – direitos do titular, com menção explícita a:	
a) possibilidade de não fornecer o consentimento, com explicação sobre as consequências da negativa, observado o disposto no § 1º do art. 6º;	
b) possibilidade de acessar os dados, retificá-los ou revogar o consentimento, por procedimento gratuito e facilitado; e	**Sugestão/ comentário:** Entendemos necessário revisar a redação deste artigo para destacar que a revogação do consentimento pode acarretar o término do serviço. Além disso, é necessário ressaltar que a retificação está relacionada apenas aos dados pessoais, não a informações gerais e principalmente opiniões ou qualquer outra forma de livre expressão.
c) possibilidade de denunciar ao órgão competente o descumprimento de disposições desta Lei.	

§ 1º Considera-se nulo o consentimento caso as informações tenham conteúdo enganoso ou não tenham sido apresentadas de forma clara, adequada e ostensiva.	
§ 2º Em caso de alteração de informação referida nos incisos I, II, III ou V do caput, o responsável deverá obter novo consentimento do titular, após destacar de forma específica o teor das alterações.	
§ 3º Em caso de alteração de informação referida no inciso IV do caput, o responsável deverá comunicar ao titular as informações de contato atualizadas.	
§ 4º Nas atividades que importem em coleta continuada de dados pessoais, o titular deverá ser informado regularmente sobre a continuidade, nos termos definidos pelo órgão competente.	
Art. 11. O consentimento será dispensado quando os dados forem de acesso público irrestrito ou quando o tratamento for indispensável para:	**Sugestão/ comentário:** o "interesse legítimo" para o tratamento de dados deve ser a principal exceção à necessidade de consentimento, pois, se ele existe, também existe uma aquiescência do titular. Isto, somado aos demais princípios desta lei, tal como finalidade e transparência, produzem um quadro normativo em linha com a evolução tecnológica e com o modelo europeu, se se apegar em aspectos formalistas que podem atravancar a livre prestação de serviços por empresas aos consumidores. **Sugestão/ comentário:** O caput do artigo 11 esclarece que o consentimento será dispensado sempre que os dados sejam de "acesso público irrestrito". A lei não define o que seria "acesso público irrestrito", o que pode gerar dúvidas sobre a sua operacionalização. Com os dados sobre salários de servidores publicados regularmente na Internet, poderiam tais dados ser considerados de acesso público irrestrito?
I – cumprimento de uma obrigação legal pelo responsável;	
II – tratamento e uso compartilhado de dados relativos ao exercício de direitos ou deveres previstos em leis ou regulamentos pela administração	**1. Sugestão/ comentário:** Esse artigo exclui a necessidade do poder público solicitar o consentimento na coleta de dados, em praticamente todas as

pública;	atividades da administração pública. Entendemos que a exceção deve ocorrer apenas no âmbito previsto no Artigo 4º. **2. Sugestão:** Além disso, sugerimos adicionar duas novas previsões: "VIII - a persecução de interesses legítimos e legais do responsável, desde que o tratamento seja feito de acordo com os princípios desta Lei e sejam preservados os direitos e garantias do titular; **§ 4º** O tratamento de dados anônimos ou de dados pessoais que tenham passado por processo de dissociação independe de consentimento, exceto no caso de dado reidentificado, que terá o tratamento de dado pessoal, nos termos desta lei.
III – execução de procedimentos pré-contratuais ou obrigações relacionados a um contrato do qual é parte o titular, observado o disposto no § 1º do art. 6º;	
IV – realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a dissociação dos dados pessoais;	
V – exercício regular de direitos em processo judicial ou administrativo;	
VI – proteção da vida ou da incolumidade física do titular ou de terceiro;	**Sugestão/ comentário:** Exclusão ou reformulação. O inciso dá margem à realização de atividades de vigilância pelo Estado sobre os indivíduos.
VII – tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias.	**Sugestão/ comentário:** Exclusão ou reformulação. O inciso dá margem à substituição do Estado na autodeterminação dos indivíduos.
§ 1º Nas hipóteses de dispensa de consentimento, os dados devem ser tratados exclusivamente para as finalidades previstas e pelo menor período de tempo possível, conforme os princípios gerais dispostos nesta Lei, garantidos os direitos do titular.	**Sugestão: § 1º** Nas hipóteses de dispensa de consentimento, os dados devem ser tratados exclusivamente para as finalidades previstas, pelo período de tempo legitimamente necessário, conforme os princípios gerais dispostos nesta Lei e garantidos os direitos do titular. **Comentário:** O período legítimo nem sempre será o mínimo.

§ 2º Nos casos de aplicação do disposto nos incisos I e II, será dada publicidade a esses casos, nos termos do parágrafo 1º do art. 6º.	
§ 3º No caso de descumprimento do disposto no §2o, o operador ou o responsável pelo tratamento de dados poderá ser responsabilizado	
Seção 2 – Dados Pessoais Sensíveis	
Art. 12. É vedado o tratamento de dados pessoais sensíveis, salvo:	
I – com fornecimento de consentimento especial pelo titular:	**Sugestão/ comentário:** Conforme mencionado anteriormente – e seguindo a orientação europeia – o consentimento para dados pessoais em geral não deve ser expresso e sim inequívoco, restando para os dados sensíveis a obrigatoriedade de consentimento expresso.
a) mediante manifestação própria, distinta da manifestação de consentimento relativa a outros dados pessoais; e	
b) com informação prévia e específica sobre a natureza sensível dos dados a serem tratados, com alerta quanto aos riscos envolvidos no tratamento desta espécie de dados; ou	
II – sem fornecimento de consentimento do titular, quando os dados forem de acesso público irrestrito, ou nas hipóteses em que for indispensável para:	
a) cumprimento de uma obrigação legal pelo responsável;	
b) tratamento e uso compartilhado de dados relativos ao exercício regular de direitos ou deveres previstos em leis ou regulamentos pela administração pública;	
c) realização de pesquisa histórica, científica ou estatística, garantida,	

sempre que possível, a dissociação dos dados pessoais;	
d) exercício regular de direitos em processo judicial ou administrativo;	
e) proteção da vida ou da incolumidade física do titular ou de terceiro;	**Sugestão/ comentário:** Exclusão ou reformulação. O inciso dá margem à realização de atividades de vigilância pelo Estado sobre os indivíduos.
f) tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias.	**Sugestão/ comentário:** Exclusão ou reformulação. O inciso dá margem à substituição do Estado na autodeterminação dos indivíduos.
§ 1º O disposto neste artigo aplica-se a qualquer tratamento capaz de revelar dados pessoais sensíveis.	
§2º O tratamento de dados pessoais sensíveis não poderá ser realizado em detrimento do titular, ressalvado o disposto em legislação específica.	Como mencionado no artigo 6.º, IX, há várias atividades que usam informações pessoais para definir um perfil de cliente para analisar os riscos. Em tais definições de perfil algumas informações pessoais podem afetar adversamente o resultado final. No entanto, a análise de risco depende de tal utilização de dados e é uma parte essencial do contexto de negócios de algumas indústrias.
§ 3º Nos casos de aplicação do disposto nos itens 'a' e 'b' pelos órgãos e entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do §1o do art. 6o.	
Art. 13. Órgão competente poderá estabelecer medidas adicionais de segurança e de proteção aos dados pessoais sensíveis, que deverão ser adotadas pelo responsável ou por outros agentes do tratamento.	**Sugestão/ comentário:** Sugestão de exclusão, em observância ao princípio da legalidade.
§ 1º A realização de determinadas modalidades de tratamento de dados pessoais sensíveis poderá ser condicionada à autorização prévia de órgão competente, nos termos do regulamento.	
§ 2º O tratamento de dados pessoais biométricos será disciplinado por	

órgão competente, que disporá sobre hipóteses em que dados biométricos serão considerados dados pessoais sensíveis.	
Seção 3 – Término do Tratamento	
Art. 14. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:	
I – verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes para o alcance da finalidade específica almejada;	**Comentário**: Considerando a tecnologia de Big Data, a finalidade precisa ser inserida dentro de um contexto moderno. Muitas vezes a finalidade surge durante o processamento de dados. **Sugestão: I** – verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes para o alcance da finalidade legítima;
II - fim do período de tratamento;	**Sugestão: II** - fim do período de tratamento, conforme definido por lei ou conforme acordado entre o responsável e o titular;
III – comunicação do titular; ou	
IV – determinação de órgão competente quando houver violação de dispositivo legal ou regulamentar.	**Sugestão**: **IV** - determinação de órgão competente quando houver violação de dispositivo legal ou regulamentar, ressalvados os princípios da razoabilidade e da proporcionalidade.
Parágrafo único. Órgão competente estabelecerá períodos máximos para o tratamento de dados pessoais, ressalvado o disposto em legislação específica.	**Comentário:** Esse é um caso em que há excesso de poder conferido à autoridade competente. A lógica deveria ser contrária: leis específicas podem prever prazos máximos a serem definidos pela autoridade competente. A definição de períodos máximos não pode ser uma regra, sob pena de por em risco a inovação. A legislação deve enfatizar a transparência da continuidade no tratamento dos dados e não um limite temporal, contrário à própria autonomia da vontade do titular. **Sugestão:** Exclusão

Art. 15. Os dados pessoais serão cancelados após o término de seu tratamento, autorizada a conservação para as seguintes finalidades:	
I – cumprimento de obrigação legal pelo responsável;	
II – pesquisa histórica, científica ou estatística, garantida, sempre que possível, a dissociação dos dados pessoais; ou	
III – cessão a terceiros, nos termos desta Lei.	
Parágrafo único. Órgão competente poderá estabelecer hipóteses específicas de conservação de dados pessoais, garantidos os direitos do titular, ressalvado o disposto em legislação específica.	**Comentário:** Se houver interesse do Estado na conservação de dados pessoais, deverá obter autorização para tal conservação por meios legais e, então, mantê-lo por sua conta. **Sugestão:** Exclusão
CAPÍTULO III – DIREITOS DO TITULAR	
Art. 16. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais, garantidos os direitos fundamentais de liberdade, intimidade e privacidade, nos termos desta Lei.	**Comentário:** Os direitos fundamentais de liberdade, intimidade e privacidade irradiam para diversos campos, não se limitando a esta lei. Sugere-se que os princípios sejam elencados no início da lei e que, nesta sessão, seja feita referência ao supra estabelecido, delegando-se ao Capítulo III os direitos decorrentes especificamente do assunto tratado, por exemplo, o direito a confirmação da existência de dados.
Art. 17. O titular dos dados pessoais tem direito a obter:	
I – confirmação da existência de tratamento de seus dados;	
II – acesso aos dados;	
III – correção de dados incompletos, inexatos ou desatualizados; e	**Comentário:** A lei deve destacar que a correção dos dados está relacionada apenas a dados pessoais, em homenagem à liberdade de expressão, de opinião e de pensamento, mesmo quando não se trate de conteúdo de cunho jornalístico.
IV – dissociação, bloqueio ou cancelamento de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei	**Comentário:** O artigo 17, IV, vale-se uma terminologia que poderia ser aperfeiçoada. A redação atual determina que “O titular dos dados pessoais

	tem direito a obter: IV – dissociação, bloqueio ou cancelamento de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei". A noção de dissociação, bloqueio ou cancelamento de dados nos quadrantes propostos pelo artigo poderia promover o exercício do chamado direito ao esquecimento em padrões cujo discernimento é dificultoso, dando margem a pedidos de dissociação, bloqueio ou cancelamento dos mais diversos. O projeto de lei nº 7881/2014, de autoria do Deputado Eduardo Cunha, recebeu diversas críticas por ordenar a remoção de links de mecanismos de buscas que apontassem para "dados irrelevantes ou defasados". Ao tutelar a dissociação, bloqueio ou cancelamento de dados desnecessários ou excessivos o APL ingressa na mesma rota de críticas recebidas pelo mencionado PL ao tratar do tema de forma perigosamente genérica. O que são dados desnecessários? E dados excessivos? Quem determina o que vem a ser necessário ou excessivo? Novamente esses são termos de fundamental importância para a implementação da lei que não foram previamente definidos e trazem para o responsável pelo tratamento dos dados uma notória insegurança sobre o que pode ser feito com os mesmos. O intuito do APL deve ser incrementar a proteção dos dados pessoais no Brasil, ao mesmo tempo em que garante a quem trata dados um conjunto de regras claras sobre os condicionantes de sua atividade. Nesse sentido, o referido dispositivo parece trazer inquietações que apenas poderiam ser superadas se a redação fosse como um todo suprimida ou apenas se deixasse a hipótese de dissociação, bloqueio e cancelamento de dados quando "tratados em desconformidade com o disposto nesta lei".
§1º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, alegando descumprimento ao disposto nesta Lei.	**Comentário:** Entendemos que este parágrafo é desnecessário e deve ser removido. O próprio direito de petição garante ao titular o poder de questionar a interpretação do responsável pelo tratamento, independente de ser ou não um caso de exceção ao consentimento, com a devida garantia

	do contraditório. Sugestão: Supressão.
§ 2º Os direitos previstos neste artigo serão exercidos mediante requerimento do titular a um dos agentes de tratamento, que adotará imediata providência para seu atendimento.	**Sugestão**: **§ 2º** Os direitos previstos neste artigo serão exercidos mediante requerimento do titular a um dos agentes de tratamento, que deverá adotar medidas para o seu cumprimento, dentro de um prazo razoável. **Comentário:** Entendemos que a palavra "imediata" pode trazer uma série de problemas do ponto de vista prático.
§ 3º Em caso de impossibilidade de adoção imediata da providência de que trata o §2o, o responsável enviará ao titular, em até sete dias a partir da data do recebimento da comunicação, resposta em que poderá:	
I – comunicar que não é agente de tratamento dos dados; ou	
II – indicar as razões de fato ou de direito que impedem a adoção imediata da providência.	
§ 4º A providência de que trata o § 2o será realizada sem ônus para o titular.	
§ 5º O responsável deverá informar aos terceiros a quem os dados tenham sido comunicados sobre a realização de correção, cancelamento, dissociação ou bloqueio dos dados, para que repitam idêntico procedimento.	
Art. 18. A confirmação de existência ou o acesso a dados pessoais serão providenciados, a critério do titular:	**Sugestão/ Comentário:** O uso de palavras como "imediatamente" no inciso I, e o termo “sete dias” previsto no inciso II dão margem a uma padronização dos temas que não leva minimamente em consideração a capacidade das empresas envolvidas. De fato, o comando “imediatamente” pode ser de fácil atendimento em determinados casos, sendo, ao contrário, materialmente impossível em outros. Da mesma forma, sete dias pode ser um prazo razoável em certas hipóteses e não ser em outras. A Abranet entende que o ideal é que a legislação abarque com razoabilidade todas as

	hipóteses, prevendo que os comandos deste artigo 18 devem ser atendidos em prazos razoáveis.
I – em formato simplificado, imediatamente; ou	
II – por meio de declaração clara e completa, que indique a origem dos dados, data de registro, critérios utilizados e finalidade do tratamento, fornecida no prazo de até sete dias, a contarem do momento do requerimento do titular.	
§ 1º Os dados pessoais serão armazenados em formato que permita o exercício do direito de acesso.	
§ 2º As informações e dados poderão ser fornecidos, a critério do titular:	**Comentário:** A Abranet entende que a lei deveria limitar-se a disciplinar o comando relativo ao direito de acesso, abstendo-se de regular os meios para seu exercício. Isso, para não impedir o livre desenvolvimento das inovações e da própria competição positiva ao consumidor que pode estimular o fornecedor a dar o melhor acesso como diferencial. Cabe à lei disciplinar o direito e exigir seu cumprimento, devendo, no entender da Abranet, abster-se de regular as formas, sob pena de engessamento do tema.
I – por meio eletrônico, seguro e idôneo para tal fim; ou	
II – sob a forma impressa, situação em que poderá ser cobrado exclusivamente o valor necessário ao ressarcimento do custo dos serviços e dos materiais utilizados.	
§ 3º - O titular poderá solicitar cópia eletrônica integral dos seus dados pessoais em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento, sempre que o banco de dados estiver em suporte eletrônico.	
§ 4º Órgão competente poderá dispor sobre os formatos em que serão fornecidas as informações e os dados ao titular.	**Sugestão/ Comentário:** A Abranet entende que a lei deveria limitar-se a disciplinar o comando relativo ao direito de acesso, abstendo-se de regular

	os meios para seu exercício. Isso, para não impedir o livre desenvolvimento das inovações e da própria competição positiva ao consumidor que pode estimular o fornecedor a dar o melhor acesso como diferencial. Cabe à lei disciplinar o direito e exigir seu cumprimento, devendo, no entender da Abranet, abster-se de regular as formas, sob pena de engessamento e superregulação do tema, de todo prejudiciais ao mercado em geral.
Art. 19. O titular dos dados tem direito a solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive as decisões destinadas a definir o seu perfil ou avaliar aspectos de sua personalidade.	**Sugestão:** Exclusão do § 1º. **Comentário**: Da forma apresentada, esse artigo viola segredos de negócios ao determinar que informações estratégicas de negócios sejam fornecidas aos usuários.
§ 1º O responsável deverá fornecer, sempre que solicitadas, informações adequadas a respeito dos critérios e procedimentos utilizados para a decisão automatizada.	
§ 2º Ficam ressalvados os tratamentos de dados pessoais necessários ao cumprimento de obrigação legal.	
Art. 20. Os dados pessoais referentes a exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.	
Art. 21. A defesa dos interesses e direitos dos titulares de dados poderá ser exercida em juízo individual ou coletivamente, na forma do disposto na Lei no 9.507, de 12 de novembro de 1997, nos arts. 81 e 82 da Lei no 8.078, de 11 de setembro de 1990, na Lei no 7.347, de 24 de julho de 1985, e nos demais instrumentos de tutela individual e coletiva.	

CAPÍTULO IV – COMUNICAÇÃO E INTERCONEXÃO	
Art. 22. Nos casos de comunicação ou interconexão de dados pessoais, o cessionário ficará sujeito às mesmas obrigações legais e regulamentares do cedente, com quem terá responsabilidade solidária pelos danos eventualmente causados.	**Sugestão/Comentário:** A responsabilidade solidária resulta em um desestímulo enorme aos negócios de processamento e *outsourcing* de dados, pois gera confusão entre os papéis desempenhados pelo responsável e pelo operador – que muitas vezes equivalem ao cedente e cessionário nesse tipo de contratação. Se o Brasil quer desenvolver o mercado de serviços nessa área, é importante que se delimite as regras aplicáveis a um e outro, afastando-se do modelo de solidariedade.
Parágrafo único. A responsabilidade solidária não se aplica aos casos de comunicação ou interconexão realizadas no exercício dos deveres de que trata a Lei no 12.527, de 18 de novembro de 2011, relativos à garantia do acesso a informações públicas.	
Art. 23. A comunicação ou interconexão de dados pessoais entre pessoas de direito privado dependerá de consentimento livre, expresso, específico e informado, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.	**Sugestão/Comentário:** Pelas razões já expostas, comunicação e interconexão poderiam formar um conceito único e mais objetivo, juntamente com transmissão e difusão. "Consentimento livre, expresso, específico e informado" deve ser substituído por "consentimento".
Art. 24. A comunicação ou interconexão de dados pessoais entre pessoa jurídica de direito público e pessoa de direito privado dependerá de consentimento livre, expresso, específico e informado do titular, salvo:	**Sugestão/ Comentário:** Pelas razões já expostas, comunicação e interconexão poderiam formar um conceito único e mais objetivo, juntamente com transmissão e difusão. "Consentimento livre, expresso, específico e informado" deve ser substituído por "consentimento".
I – nas hipóteses de dispensa do consentimento previstas nesta Lei;	
II – nos casos de uso compartilhado de dados previsto no inciso XVII do art. 5º, em que será dada publicidade nos termos do §1º do art. 6º; ou	**Sugestão/ Comentário:** Como mencionado nos comentários em outros artigos, a dispensa de autorização para entidades públicas, no entender da Abranet, está muito ampla, sendo necessário sua especificação para

	garantia dos usuários em geral. Haverá casos em que, por exemplo, o tratamento será conjunto, entre entes públicos e privados, inviabilizando a dualidade de regimes.
III – quando houver prévia autorização de órgão competente, que avaliará o atendimento ao interesse público, a adequação e a necessidade da dispensa do consentimento.	
Parágrafo único. A autorização prevista no inciso III do caput poderá ser condicionada:	
I – à comunicação da interconexão aos titulares, nos termos do §1º do art. 6º;	
II – ao oferecimento aos titulares de opção de cancelamento de seus dados; ou	
III – ao cumprimento de obrigações complementares determinadas por órgão competente.	
Art. 25. A comunicação ou interconexão entre órgãos e entidades de direito público será objeto de publicidade, nos termos do §1º do art. 6º, e obedecerá às regras gerais deste Capítulo.	
Art. 26. O órgão competente poderá solicitar, a qualquer momento, aos órgãos e entidades públicos que realizem interconexão de dados e o uso compartilhado de dados pessoais, informe específico sobre o âmbito, natureza dos dados e demais detalhes do tratamento realizado, podendo emitir recomendações complementares para garantir o cumprimento desta Lei.	
Art. 27. Órgão competente poderá estabelecer normas complementares para as atividades de comunicação e interconexão de dados pessoais.	**Sugestão / Comentário:** Remoção do dispositivo ou reformulação, para atender ao princípio da legalidade.

CAPÍTULO V – TRANSFERÊNCIA INTERNACIONAL DE DADOS	
Art. 28. A transferência internacional de dados pessoais somente é permitida para países que proporcionem nível de proteção de dados pessoais equiparável ao desta Lei, ressalvadas as seguintes exceções:	**Comentário:** O modelo adotado neste artigo, de adequação entre diferentes legislações tem se provado, na Europa, ineficiente e burocrático, tornando casuísticas as exceções em alguns casos. Em outros, o reconhecimento da adequação da legislação não leva em consideração se há medidas práticas que garantam sua aplicação. Por esses motivos, 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, independente de onde os dados pessoais sejam tratados. O importante é a responsabilidade do responsável diante do titular. Vale ressaltar que existem diversos modelos normativos de transferência de dados que são aceitos internacionalmente. A legislação brasileira, em prol da simplicidade, clareza e reconhecimento da tendência de tratamento de dados em nível global, deve reconhecer os modelos compatíveis e facultar aos responsáveis pelo tratamento a adoção de qualquer desses modelos.
I – 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;	
II – quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;	
III – quando órgão competente autorizar a transferência, nos termos de regulamento;	
IV – quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;	
V – quando a transferência for necessária para execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos	

do §1º do art. 6º.	
Parágrafo único. O nível de proteção de dados do país será avaliado por órgão competente, que levará em conta:	
I – normas gerais e setoriais da legislação em vigor no país de destino;	
II – natureza dos dados;	
III – observância dos princípios gerais de proteção de dados pessoais previstos nesta Lei;	
IV – adoção de medidas de segurança previstas em regulamento; e	
V – outras circunstâncias específicas relativas à transferência.	
Art. 29. Nos casos de países que não proporcionem nível de proteção equiparável ao desta Lei, o consentimento de que trata o art. 7º será especial, fornecido:	**Sugestão:** A Abranet sugere a elaboração de uma exceção para os casos de transferência interna das empresas.
I – mediante manifestação própria, distinta da manifestação de consentimento relativa a outras operações de tratamento; e	
II – com informação prévia e específica sobre o caráter internacional da operação, com alerta quanto aos riscos envolvidos, de acordo com as circunstâncias de vulnerabilidade do país de destino.	
Art. 30. A autorização referida no inciso III do caput do art. 28 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 para uma transferência específica, em cláusulas contratuais-padrão ou em normas corporativas globais, nos termos do regulamento.	**Sugestão/Comentário:** A Abranet sugere que a adoção de cláusulas-padrão ou de modelos internacionais reconhecidos pelo Brasil deve ser excludente de qualquer outra exigência e suficiente para validar a transferência.
§ 1º Órgão competente poderá elaborar cláusulas contratuais-padrão, que deverão observar os princípios gerais de proteção de dados e os direitos do titular, garantida a responsabilidade solidária, independente de culpa, de cedente e cessionário.	**Sugestão/Comentário** : A Abranet sugere que a responsabilidade seja definida de acordo com a culpabilidade do agente, sem solidariedade, ou que esta seja exceção.

§ 2º Os responsáveis pelo tratamento que fizerem parte de um mesmo grupo econômico ou conglomerado multinacional poderão submeter normas corporativas globais à aprovação de órgão competente, obrigatórias para todas as empresas integrantes do grupo ou conglomerado, a fim de obter permissão para transferências internacionais de dados dentro do grupo ou conglomerado sem necessidade de autorizações específicas, observados os princípios gerais de proteção e os direitos do titular.	**Sugestão/Comentário**: A Abranet sugere o reconhecimento das regras já estabelecidas internacionalmente, como modelos já existentes na União Europeia e na Ásia.
§ 3º Na análise de cláusulas contratuais ou de normas corporativas globais submetidas à aprovação de órgão competente, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento.	**Sugestão/Comentário**: A Abranet reitera seu comentário ao item anterior, para que sejam reconhecidos mecanismos já existentes.
Art. 31. O cedente e o cessionário têm responsabilidade solidária pelo tratamento de dados realizado no exterior ou no território nacional, em qualquer hipótese, independente de culpa.	**Sugestão/Comentário** : Conforme comentários em outros incisos, a Abranet entende necessário que se estabeleça um regime de responsabilidade que leve em conta as diversas situações envolvidas, bem como que estabeleça as devidas excludentes de responsabilidade.
Art. 32. No caso de transferência internacional de dados de país estrangeiro para o Brasil, somente é permitido o seu tratamento no território nacional quando nas operações realizadas naquele país tiverem sido observadas suas normas relativas à obtenção de consentimento.	
Art. 33. Órgão competente poderá estabelecer normas complementares que permitam identificar uma operação de tratamento como transferência internacional de dados pessoais.	**Sugestão/Comentário** : Exclusão ou reformulação, para detalhamento e enquadramento ao princípio da legalidade.
CAPÍTULO VII – RESPONSABILIDADE DOS AGENTES	
Seção I – Agentes do Tratamento e Ressarcimento de Danos	
Art. 34. São agentes do tratamento de dados pessoais o responsável e o operador.	

Art. 35. Todo aquele que, por meio do tratamento de dados pessoais, causar a outrem dano material ou moral, individual ou coletivo, é obrigado a ressarci-lo.	**1. Sugestão/Comentário** : A Abranet entende que o "responsável" é o principal agente do tratamento de dados, devendo responsabilizar-se por seus atos, salvo excludentes, tal como a culpa exclusiva de terceiros. O operador do tratamento ou algum terceiro poderia sofrer responsabilidade mesmo atuando apenas seguindo instruções do responsável. No entender da Abranet, o artigo deveria contemplar tais situações, para que se tenham regras cristalinas.
§ 1º 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 excessivamente onerosa;	
§ 2º O responsável ou o operador podem deixar de ser responsabilizados se provarem que o fato que causou o dano não lhes é imputável.	
Art. 36. 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. 37. As punições cabíveis no âmbito desta Lei serão aplicadas pessoalmente aos operadores e responsáveis de órgãos públicos que agirem de forma contrária a esta Lei, 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. 38. As competências e responsabilidades relativas à gestão de bases de dados nos órgãos e entidades públicos, bem como a responsabilidade pela prática de atos administrativos referentes a dados pessoais, serão definidas nos atos normativos que tratam da definição de suas competências.	
Seção II – Responsável e Operador	
Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo responsável, que verificará a observância das próprias instruções e das normas sobre a matéria.	

§ 1º O responsável tem responsabilidade solidária quanto a todas as operações de tratamento realizadas pelo operador	**Sugestão/Comentário**: Conforme expresso no artigo 35, a Abranet sugere uma revisão e melhor esclarecimento do regime de responsabilidade. O operador não deve ser responsabilizado se agir em conformidade com as orientações do responsável.
§ 2º Órgão competente poderá determinar ao responsável que elabore relatório de impacto à privacidade referente às suas operações de tratamento de dados, nos termos do regulamento.	
Art. 40. O responsável ou o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, observado o disposto no art. 15.	
Parágrafo único. Órgão competente poderá dispor sobre formato, estrutura e tempo de guarda do registro.	**Sugestão / Comentário**: Preliminarmente, a Abranet faz referência aos seus comentários ao artigo 1º , onde procurou esclarecer que as informações fornecidas nesta lei sobre a atuação de uma "autoridade" são escassas e não permitem a plena contribuição e, ao mesmo tempo, deixar claro o que entende como premissas mínimas para existência de autoridade. Em segundo lugar, Abranet entende que a lei deveria limitar-se a disciplinar o comando relativo ao direito em questão, abstendo-se de regular os formatos para sua entrega. Isso, para não impedir o livre desenvolvimento das inovações e da própria competição positiva ao consumidor que pode estimular o fornecedor a dar o melhor acesso como diferencial. Cabe à lei disciplinar o direito e exigir seu cumprimento, devendo, no entender da Abranet, abster-se de regular as formas, sob pena de engessamento e superregulação do tema, de todo prejudiciais ao mercado em geral.
Seção III – Encarregado pelo Tratamento de Dados Pessoais	
Art. 41. O responsável deverá indicar um encarregado pelo tratamento de dados pessoais.	

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente de forma clara e objetiva, preferencialmente na página eletrônica do responsável na Internet.	**Sugestão/Comentário**: Por questões de segurança, a Abranet sugere que outros meios de contato devem ser previstos que não o contato direto com o encarregado.
§ 2º As atividades do encarregado consistem em:	
I – receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;	
II – receber comunicações do órgão competente e adotar providências;	
III – orientar os funcionários da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e	
IV – demais atribuições estabelecidas em normas complementares ou determinadas pelo responsável.	**Sugestão/Comentário** : A Abranet entende que tais disposições deveriam ser apenas diretrizes e não regras. As empresas devem ter a liberdade para se organizarem de acordo com o seu modelo de negócio. O papel do encarregado pode variar muito dependendo da natureza da atividade (startup, bancos, indústria). Além disso, o poder discricionário dado à autoridade competente pode fazer com que, sem o devido debate no Legislativo, uma autoridade crie novas normas limitadoras de atividades lícitas.
§ 3º Órgão competente estabelecerá normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de definição, conforme critérios de natureza ou porte da entidade, e volume de operações de tratamento de dados.	
Seção IV – Segurança e Sigilo de Dados	
Art. 42. O operador deve adotar medidas de segurança técnicas e administrativas constantemente atualizadas, proporcionais à natureza das	

informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação, difusão, ou qualquer forma de tratamento inadequado ou ilícito.	
Parágrafo único. As medidas de segurança devem ser compatíveis com o atual estado da tecnologia, com a natureza dos dados e com as características específicas do tratamento, em particular no caso de dados sensíveis.	
Art. 43. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se ao dever de sigilo em relação aos dados pessoais, mesmo após o seu término.	
Art. 44. O responsável deverá comunicar imediatamente ao órgão competente a ocorrência de qualquer incidente de segurança que possa acarretar prejuízo aos titulares.	**Sugestão/Comentário**: Inicialmente, os incidentes deverão ser avaliados conforme o potencial de causar danos ou danos efetivamente causados. Não é desejável que incidentes sem consequências ou riscos sem potencial de danos efetivos sejam tratados da mesma forma que os incidentes efetivamente relevantes. Incidentes acontecem a todo o momento e a autoridade competente deve se encarregar daqueles relevantes, sob pena de perda e desperdício de recursos. A notificação imediata à autoridade não é viável, pois, investigar uma ameaça leva tempo e determinar se alguma informação foi comprometida também. Seria melhor dizer "assim que o controlador tenha determinado o incidente pode representar um risco/ameaça, etc ..."
Parágrafo único. A comunicação deverá mencionar, no mínimo:	
I – descrição da natureza dos dados pessoais afetados;	
II – informações sobre os titulares envolvidos;	
III – indicação das medidas de segurança utilizadas para a proteção dos	

dados, inclusive procedimentos de encriptação;	
IV – riscos relacionados ao incidente; e	
V – medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos de prejuízo.	
Art. 45. Órgão competente poderá determinar a adoção de providências quanto a incidentes de segurança relacionados a dados pessoais, conforme sua gravidade, tais como:	
I – pronta comunicação aos titulares;	
II – ampla divulgação do fato em meios de comunicação; ou	
III – medidas para reverter ou mitigar os efeitos de prejuízo.	
§ 1º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis para terceiros não autorizados a acessá-los.	
§ 2º A pronta comunicação aos titulares afetados pelo incidente de segurança será obrigatória, independente de determinação do órgão competente, nos casos em que for possível identificar que o incidente coloque em risco a segurança pessoal dos titulares ou lhes possa causar danos.	
Art. 46. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos princípios gerais previstos nesta Lei e às demais normas regulamentares.	
Art. 47. Órgão competente poderá estabelecer normas complementares acerca de critérios e padrões mínimos de segurança, inclusive com base na evolução da tecnologia.	**Sugestão/Comentário**: Com as ressalvas feitas ao artigo primeiro desta contribuição, a Abranet entende que à hipotética autoridade competente não seria recomendável estabelecer critérios técnicos, na medida em que estes certamente se tornarão obsoletos em um curto prazo de tempo.
Seção V – Boas Práticas	

Art. 48. Os responsáveis pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas que estabeleçam condições de organização, regime de funcionamento, procedimentos, normas de segurança, padrões técnicos, obrigações específicas para os diversos envolvidos no tratamento, ações formativas ou mecanismos internos de supervisão, observado o disposto nesta Lei e em normas complementares sobre proteção de dados.	
Parágrafo único. As regras de boas práticas disponibilizadas publicamente e atualizadas poderão ser reconhecidas e divulgadas pelo órgão competente.	
Art. 49. O órgão competente estimulará a adoção de padrões técnicos para softwares e aplicações de Internet que facilitem a disposição dos titulares sobre seus dados pessoais, incluindo o direito ao não rastreamento.	**Sugestão/Comentário**: A Abranet sugere a remoção deste artigo na medida em que não foi possível contribuir com sugestões de alteração por não existirem maiores explicações sobre a natureza de tais critérios. Importante notar que atualmente a leitura feita pela Abranet é que representa uma imposição de padrões técnicos, o que é questionável, *vis a vis* a velocidade da inovação e da competição. Novamente a Abranet sugere que a regulamentação estabeleça os direitos, e permita que a indústria desenvolva os meios.
CAPÍTULO VIII – SANÇÕES ADMINISTRATIVAS	
Art. 50. As infrações realizadas por pessoas jurídicas de direito privado às normas previstas nesta Lei ficam sujeitas às seguintes sanções administrativas aplicáveis por órgão competente:	
I – multa simples ou diária;	**Sugestão/Comentário**: A Abranet sugere a fixação de critérios para aplicação da multa, bem como o estabelecimento de um teto, com fundamento nos princípios da administração pública . Além disso, é possível que a mera advertência seja prevista como sanção, para casos em que ocorrerem infrações de menor potencial de causar danos.

II – publicização da infração;	
III – dissociação dos dados pessoais;	
IV – bloqueio dos dados pessoais;	
V – suspensão de operação de tratamento de dados pessoais, por prazo não superior a dois anos;	
VI – cancelamento dos dados pessoais;	
VII – proibição do tratamento de dados sensíveis, por prazo não superior a dez anos; e	
VIII – proibição de funcionamento de banco de dados, por prazo não superior a dez anos.	
§ 1º As sanções poderão ser aplicadas cumulativamente.	
§ 2º Os procedimentos e critérios para a aplicação das sanções serão adequados em relação à gravidade e à extensão da infração, à natureza dos direitos pessoais afetados, à existência de reincidência, à situação econômica do infrator e aos prejuízos causados, nos termos do regulamento.	**Sugestão/Comentário**: Deve haver espaço para qualificadores positivos aqui, como a existência de um programa abrangente de privacidade, a velocidade de introdução de fatores de correção, a ausência de intencionalidade. - Multas razoáveis são uma parte fundamental de qualquer regime sólido de proteção de dados. - No entanto, o fato de que o projeto de lei é aplicável a todos os setores e tamanhos de negócios exige uma abordagem diferenciada e equilibrada. - Também é importante para evitar que o elevado nível de sanções possa minar o incentivo das empresas para investir no Brasil, - Pode também criar um desincentivo para o envolvimento das empresas com os órgãos reguladores.
§ 3º Os prazos de proibição previstos nos incisos VII e VIII do caput poderão ser prorrogados pelo órgão competente, desde que verificada a omissão no cumprimento de suas determinações, a reincidência no cometimento de infrações ou a ausência de reparação integral de danos causados pela infração.	

§ 4º O disposto neste artigo não prejudica a aplicação de sanções administrativas, civis ou penais definidas em legislação específica.	
§ 5º O disposto nos incisos III a VII poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei no 8.112, de 11 de dezembro de 1990 e na Lei no 8.429, de 2 de junho de 1992	
CAPÍTULO IX – DISPOSIÇÕES TRANSITÓRIAS E FINAIS	
Art. 51. Órgão competente estabelecerá normas sobre adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, considerada a complexidade das operações de tratamento, a natureza dos dados e o porte do responsável.	
Art. 52. Esta Lei entrará em vigor no prazo de 120 (cento e vinte) dias contados da data da sua publicação.	**Sugestão/Comentário** : O prazo não será suficiente para a adequação das empresas, sugerimos o aumento para ao menos um ano e preferencialmente dois, como em outros países.