Comentários do Centre for Information Policy Leadership sobre o Anteprojeto revisado da Lei de Privacidade do Brasil

O Centre for Information Policy Leadership (CIPL)[1] pelo presente documento envia comentários sobre o anteprojeto revisado da lei de privacidade do Brasil (projeto de lei que prevê o processamento de dados pessoais para garantir o livre desenvolvimento da personalidade e dignidade da pessoa natural) divulgado em outubro de 2015.

Em abril de 2015, o CIPL enviou comentários[2] sobre a primeiro versão deste anteprojeto, que foi divulgado em janeiro de 2015. Agradecemos imensamente a oportunidade de complementar os nossos comentários anteriores com algumas observações adicionais sobre a nova versão.

Desde a divulgação do primeiro anteprojeto, nós não fornecemos apenas as informações por escrito referidas acima sobre o processo do Brasil para desenvolver uma lei de privacidade abrangente, mas também conversamos com uma série de importantes partes interessadas brasileiras, incluindo formuladores de políticas e legisladores envolvidos no desenvolvimento desta importante lei, bem como representantes da indústria, sociedade civil e academia. Coordenamos reuniões da delegação com importantes stakeholders e organizamos uma conferência de privacidade global em Brasília em outubro 2015 conjuntamente com o Instituto Brasiliense de Direito Público. Agradecemos muito o nível de interesse e a receptividade às nossas ideias que os interlocutores brasileiros demonstraram em todos os momentos.

Iniciamos nossos comentários e observações adicionais abaixo elogiando os autores pelas muitas melhorias que são evidentes no projeto de lei revisado. Eles incluem o conceito de "interesse legítimo" como base para a legitimação do processamento de dados, a definição e a aplicação mais flexíveis de "consentimento", a inclusão de conceitos de gestão de risco de privacidade em "melhores práticas", a capacidade de a indústria utilizar os dados para fins de pesquisa, o esforço

[1] O CIPL é uma think tank especializada em segurança e privacidade global do escritório de advocacia Hunton & Williams, estabelecido há mais de 12 anos. Conta com o apoio de aproximadamente 38 empresas membros que são líderes nos principais setores da economia global. O CIPL oferece experiência e liderança sobre problemas de política global de segurança e privacidade, trabalha com diretores de privacidade, órgãos reguladores e especialistas externos para desenvolver melhores práticas e garantir eficácia na proteção de privacidade e gestão de informações na era moderna de informações. Para obter mais informações, consulte o website do Centro em http://www.informationpolicycentre.com/. Nenhuma informação contida no presente comentário será interpretada como representação de opinião de nenhum membro individual do Centro nem do escritório de advocacia Hunton & Williams LLP.

[2] Comentários disponíveis em: https://www.informationpolicycentre.com/files/Uploads/Documents/Centre/Comments_Centre_for_Information_Policy_Leadership_Brazil_draft_law.pdf; e https://www.informationpolicycentre.com/files/Uploads/Documents/Centre/Comentarios_do_Centre_for_Information_Policy_Leadership_Anteprojeto_de_lei_do_Brasil.pdf.

para elaborar uma norma adequada de “anonimização” para remover os dados pessoais do âmbito da presente lei e outras características. Tudo isso contribuirá para que o Brasil elabore uma lei de privacidade que será adequada para a economia e sociedade moderna orientadas por dados e permitirá proteções e inovação eficazes da privacidade.

No entanto, para atingir esse objetivo, acreditamos que algumas áreas precisam de mais esclarecimento e refinamento. Tentaremos manter breves nossas sugestões sobre estes pontos, direcionando, em parte, aos nossos comentários anteriores onde já abordaram o problema, e, por outro lado, convidando-o a buscar mais esclarecimentos conosco, quando necessário. Observe também que os nossos comentários são baseados em uma combinação de variadas e, às vezes, divergentes versões do texto traduzido para o inglês, o que pode ter provocado algum mal-entendido quanto à intenção ou ao sentido real em alguns contextos.

I. Comentários adicionais

Interesse legítimo

É com satisfação que acolhemos a inclusão do “interesse legítimo” como base para o processamento entre várias alternativas que incluem também o consentimento. Consideramos este um passo significativo para permitir os usos da informação moderna, em que o consentimento nem sempre é viável ou possível.

No entanto, sugerimos alguns esclarecimentos. O Artigo 10(1) parece prever que na aplicação da norma de interesse legítimo, deve-se considerar as "expectativas legítimas" do titular dos dados nos termos do Artigo 6(II), que prevê que todo o processamento (e não apenas o processamento de interesse legítimo) deva ser compatível com as expectativas legítimas do titular dos dados.

Um dos valores do processamento de interesse legítimo é que ele permite o processamento posterior para fins que, anteriormente, eram desconhecidos, inimagináveis e inesperados, como no caso de dados coletados para um propósito, mas que agora descobriu-se serem úteis para facilitar uma finalidade diferente. Se as “expectativas legítimas” do titular dos dados no momento da coleta original forem o teste para saber se o processamento para o novo propósito pode seguir adiante, o processamento baseado em interesse legítimo não servirá para seu propósito nem acrescentará nada de novo.

A proteção do titular dos dados no contexto de processamento baseado em interesse legítimo resulta do fato de que os interesses comerciais em jogo devem ser ponderados com base nos possíveis danos aos direitos e às liberdades fundamentais do indivíduo, como o projeto de lei já prevê corretamente. Em vista disto, não está claro por que a exigência adicional de “expectativas razoáveis” é necessária e, de fato, parece minar a base do interesse legítimo para processamento. Portanto, recomendamos que a versão final da lei esclareça esse ponto e exclua “expectativas legítimas” do teste de “interesse legítimo”. Dessa forma, o Artigo 10 pode ser alterado para o seguinte: “O processamento baseado no interesse legítimo do controlador dos dados será válido se o interesse legítimo indicado não for superado pelos danos aos direitos e liberdades

individuais, relacionados a uma situação concreta e o processamento for necessário para a finalidade pretendida".

Consentimento

No anteprojeto revisado, o consentimento, aparentemente, deve ser "expresso" apenas em relação ao processamento de dados sensíveis (Artigo 11(I)). A definição geral de consentimento no Artigo 5(VII) já não inclui uma exigência de que o consentimento deva ser expresso. O Artigo 7 também se refere a consentir apenas como tendo que ser "livre e inequívoco", e apenas o Artigo 11(I) relativo ao processamento de dados pessoais sensíveis requer consentimento "expresso e específico". O Artigo 9 explica sobre a definição geral de consentimento o seguinte: "O consentimento previsto no art 7º, I deverá ser livre e inequívoco e fornecido por escrito ou *por meio de qualquer outro meio que o certifique*". (Grifo nosso) Isto sugere que, em algumas circunstâncias o consentimento "presumido" e o consentimento "implícito" (bem como outras formas de demonstração de consentimento) podem ser adequados nos termos desta lei, desde que essas formas de consentimento "demonstrem" suficientemente a intenção do indivíduo, o que ele pode se a não presunção, por exemplo, acompanha um aviso claro e efetivo da opção de presumir.

Concordamos em fornecer o consentimento presumido ("opt-out"), o consentimento implícito e outras formas de demonstração de consentimento em contextos adequados, uma vez que reflete uma recomendação que tínhamos feito em nossos comentários anteriores para a primeira verssão do anteprojeto. Por alguns dos mesmos motivos que o "interesse legítimo" é uma alternativa necessária para processamento baseado em consentimento no contexto de análise de grandes volumes de dados (big data) e outros usos modernos de informações, a definição de "consentimento" propriamente dita deve ser mais ampla e mais flexível do que o termo "consentimento expresso" permite. Em alguns contextos, os indivíduos podem indicar claramente suas intenções ou o consentimento por apenas "não agir", por exemplo, por não "opt-out" para determinados usos de suas informações pessoais. Intimamente relacionada a isso está a ideia de que o consentimento pode ser implícito a partir de ações (ou inércias) de indivíduos em determinados contextos. Acreditamos que a atual versão do anteprojeto prevê a flexibilidade necessária específica ao contexto sobre a forma adequada de consentimento. No entanto, vimos também versões divergentes do texto traduzido para o inglês do Artigo 9, o que causa alguma confusão sobre a intenção deste artigo. Na medida em que o texto original em português também está sujeito a interpretações divergentes, recomendamos que ele seja esclarecido.

Boas práticas

Também acolhemos com satisfação a incorporação do conceito de gestão de risco de privacidade por responsáveis pelo tratamento e operadores no desenvolvimento de normas de melhores práticas na Seção II, Artigo 50(1), prevendo que no desenvolvimento de tais normas, "levarão em consideração a natureza, escopo e finalidade do tratamento e dos dados, bem como a probabilidade e gravidade dos riscos de danos aos indivíduos". O reconhecimento explícito no anteprojeto atual de uma abordagem baseada em risco para a elaboração e implementação de proteções de privacidade é fundamental para inovação e uma moderna economia da informação. Qualquer lei de proteção de dados capaz de resistir ao teste do tempo deve ser sensível ao fato de

que diferentes tipos de dados e de processamento podem apresentar diferentes níveis de risco e, portanto, requerem diferentes respostas de conformidade e níveis de mitigações.

A título de esclarecimento adicional, recomendamos que a lei final não somente exija a consideração de risco no contexto de "formular regras de boas práticas", mas também na implementação e aplicação dessas regras nas atividades diárias de tratamento dos responsáveis e operadores.

Além disso, sugerimos a incorporação explícita do conceito de avaliação dos benefícios de tratamento de dados para o titular dos dados, a organização e a sociedade em qualquer quadro de avaliação ou gestão de risco. Embora isso esteja implícito no texto atual de "levarão em consideração a natureza, escopo e finalidade do tratamento...", gostaríamos de acrescentar os termos "benefícios ao indivíduo, à organização e à sociedade" a esta lista de considerações para serem ponderados em relação aos riscos.

Por fim, pensamos que os objetivos dessas "boas práticas" seriam significativamente respaldados se a lei especificasse os incentivos para as organizações criarem e implementarem essas regras de boas práticas. Por exemplo, empresas que demonstraram sua responsabilidade ao participar dessas regras poderiam receber maior liberdade para utilizar dados pessoais para uma gama mais ampla de finalidades legítimas e benéficas, sujeita à prevenção de danos aos indivíduos.[3]

Dados anônimos

A importância da anonimização dos dados pessoais como uma ferramenta para excluir esses dados desta lei visando permitir uma ampla gama de usos benéficos dos dados, como análise de grandes volumes de dados (big data) para fins de pesquisa científica, melhoria de produtos e desenvolvimento, não pode ser menosprezada. O anteprojeto de lei reconhece claramente esse fato na medida em que deixa claro que ele se aplica apenas ao tratamento de "dados pessoais", que são dados sobre uma pessoa identificada ou identificável, e não a "dados anonimizados", o que significa dados que "não possa ser identificado". (Artigo 5(IV))

No entanto, o anteprojeto também prevê que onde a anonimização é revertida ou reversível "com esforços razoáveis", esses dados estariam sujeitos à lei. (Artigo 13) Reconhecemos e entendemos que a anonimização que pode ser revertida representa um risco aos titulares dos dados. Por outro lado, as empresas devem ser incentivadas a tentar anonimizar os dados, pois reduz o risco para os titulares dos dados. No entanto, sujeitar as empresas a um nível extremamente difícil de prever se uma técnica de anonimização "pode" ser razoavelmente reversível fornece pouco incentivo para as organizações e tem pouca utilidade prática. Portanto, apoiamos uma abordagem de duas vertentes: Primeiro, os dados anonimizados não devem ser abrangidos pela presente lei, onde a desanonimização (ou reidentificação) pode ser realizada somente por meio de esforços

[3] Para obter uma explicação detalhada sobre este conceito, consulte um white paper recente da CIPL sobre "O papel da responsabilidade aprimorada para criar uma sociedade sustentável de informações e economia orientadas por dados" disponível em: https://www.informationpolicycentre.com/files/Uploads/Documents/Centre/World_of_Big_Data_Accountability_and_Digital_Responsibility_Sustainable_Data-Driven_Economy_and_Information_Society.pdf.

extraordinários (em vez de "razoáveis"). Em segundo lugar, nos casos em que os dados anonimizados podem ser desanonimizados por meio de esforços "razoáveis", acreditamos que ainda devam ser considerados anônimos para efeitos da presente lei, **se** a anonimização for vinculada a proteções processuais, administrativas e legais adicionais com base na desanonimização ou reidentificação. Portanto, recomendamos que o anteprojeto também incorpore proteções processuais, administrativas e jurídicas, como compromissos contratuais executáveis para não reidentificar os dados anonimizados, bem como proibições legais para não fazê-lo, para garantir que todos os dados anonimizados possam ser reconhecidos como tal e excluídos nos termos da lei.[4]

Além disso, a cláusula "com esforços razoáveis" do Artigo 13 levanta a questão do que é qualificado como um esforço "razoável" para desanonimizar e o que é um esforço extraordinário. O Artigo 13(2) do anteprojeto prevê que o órgão público competente "poderá dispor sobre padrões e técnicas utilizadas em processos de anonimização". Recomendamos que, na medida em que a cláusula "com esforços razoáveis" for mantida, o Artigo 13(2) esclareça que o órgão competente também pode fornecer parâmetros adequados para a questão do que constitui esforços razoáveis e extraordinários relativos à desanonimização.

Acreditamos que sem incorporar proteções processuais, administrativas e jurídicas à análise para determinar se os dados descaracterizados são suficientemente anônimos para removê-los do escopo da presente lei e sem prever o estabelecimento de um padrão viável de "razoabilidade", seria quase impossível em um número crescente de casos obter a "anonimização" para fins de exclusão de dados pessoais desta lei.

Além disso, os dados anônimos, por vezes, devem ser reidentificados para proporcionar os benefícios aos indivíduos derivados das percepções obtidas por meio da análise de dados anonimizados. Assim, a lei deve prever padrões razoáveis para a reidentificação, se for o caso, ou permitir a reidentificação nos casos em que as exigências de interesse legítimo forem atendidas. A necessidade de reidentificação em alguns contextos é outra razão para as medidas complementares de anonimização técnica com medidas processuais, administrativas e jurídicas para permitir o tratamento de dados descaracterizados como "anonimizados" para efeitos da presente lei, mesmo quando eles podem ser razoavelmente reidentificados sem esforços extraordinários.

Definição de Pesquisa

Lidos juntos, o Artigo 7(IV) e o Artigo 11(II)(c) e §3º, indicam que a "pesquisa" como base para tratamento nos termos do Artigo 7 também se aplica à pesquisa realizada pelo setor comercial,

[4] Para obter uma explicação sobre esta abordagem, *consulte, por exemplo,* o Relatório FTC - EUA, "Protecting Consumer Privacy in an Era of Rapid Change – Recommendations for Business and Policymakers" (Protegendo a privacidade do consumidor em uma era de rápidas mudanças – recomendações para empresas e políticos) 2012, *disponível em*: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf; *consulte também* "Anonymization and Risk" (Anonimização e risco) por Ira Rubinstein e Woodrow Hartzog, *disponível em:* http://papers.ssrn.com/sol3/abstract_id=2646185.

sujeita à anonimização quando possível. Isso também implica o fato de essa pesquisa poder ser realizada sem consentimento, uma vez que nos termos do Artigo 11 §3º, a pesquisa realizada nos dados confidenciais exclui explicitamente a pesquisa comercial sem o consentimento expresso.

Concordamos que o termo *pesquisa* geralmente deva abranger a pesquisa realizada por entidades do setor privado para fins comerciais, mas também estenderia essa capacidade no caso de dados confidenciais, especialmente quando eles estão sendo administrados em conformidade com um regime de anonimização adequada e eficaz (e reidentificação). A pesquisa científica do setor privado para fins médicos, por exemplo, não deve ser excluída quando a informação racial ou étnica, ou os dados relativos à saúde, à vida sexual e à informação genética ou biométrica podem ser diretamente relevantes para o estudo.

Além disso, a anonimização como parece ser concebida atualmente no anteprojeto de lei não parece ser uma solução, porque em tais contextos, a reidentificação deve ser uma possibilidade. No entanto, atualmente, a capacidade de reidentificação de informações parece excluir o status de dados "anonimizados" nos termos do anteprojeto de lei. Recomendamos, portanto, que a questão da pesquisa do setor privado seja reconsiderada e esclarecida.

Jurisdição

O Artigo 3 do anteprojeto revisado prevê essencialmente que a lei se aplica a qualquer operação de tratamento, independentemente de onde o operador esteja sediado ou de onde os dados estejam localizados, se (1) o processamento ocorrer no Brasil; ou (2) o processamento tiver como objetivo fornecer bens ou serviços a pessoas localizadas no Brasil ou envolver o processamento de dados de pessoas localizadas no Brasil; ou (3) os dados foram coletados no Brasil.

Acreditamos que esta declaração de jurisdição deva ser refinada para tornar claro que os responsáveis pelo tratamento de dados estrangeiros não estejam sujeitos à lei de privacidade brasileira quando eles estiverem usando operadores brasileiros para tratar dados que não são brasileiros no Brasil. A imposição da lei de privacidade brasileira sobre os responsáveis estrangeiros criaria entraves significativos para o setor de serviços de TI do Brasil, bem como para outros operadores no Brasil que prestam serviços para clientes globais. Os operadores brasileiros que tratam dados em nome de seus clientes estrangeiros devem poder aplicar a lei estrangeira pertinente aos dados no ponto de coleta. Assim, por exemplo, se um operador brasileiro tratar dados em nome de um responsável japonês, ele deverá poder aplicar as exigências legais japonesas pertinentes a esses dados, em vez da lei brasileira. Aplicação do Artigo 3(1) a esse tratamento de dados no Brasil minaria e incapacitaria drasticamente qualquer setor detratamento brasileiro que quisesse prestar serviços a clientes globais.

Além disso, a linguagem do anteprojeto atual é pouco clara no que diz respeito ao significado de "pessoas situadas no" Brasil. Para evitar cenários absurdos de jurisdição relacionados a visitantes e turistas, talvez a cláusula pudesse ser esclarecida para se referir a residentes permanentes e cidadãos brasileiros domiciliados no Brasil no momento da coleta ou do processamento.

Em suma, em nossa opinião, a jurisdição da lei de privacidade sobre responsáveis deve se estender apenas aos responsáveis estabelecidos e/ou localizados no Brasil ou aos responsáveis

que estão localizados fora do Brasil, mas que estão direcionando seus serviços aos residentes no Brasil e coletando propositadamente dados pessoais de quem reside no Brasil.

Transferências internacionais

Estamos contentes com a inclusão do consentimento como uma base para legitimar as transferências de dados transfronteiriças. (Artigo 33(VII).

No entanto, como discutimos em nossos comentários sobre o anteprojeto anterior deste projeto de lei, consideramos importante que qualquer regime legal para transferências transfronteiriças deva ser capaz de interagir e refletir toda a gama de mecanismos de transferência transfronteiriça disponíveis em outras jurisdições e regiões. Assim, torna-se possível que as organizações globais elaborem uma abordagem global coerente, eficiente e sem atrito em relação às transferências transfronteiriças de dados pessoais.

Parece que apesar de permitirem normas corporativas globais de estilo europeu (EU Binding Corporate Rules - BCR (Regras de Privacidade Vinculativas da Empresa UE), os mecanismos de transferência transfronteiriça incluídos atualmente no anteprojeto de lei ainda não refletem mecanismos como as APEC Cross Border Privacy Rules - CBPR (Regras de Privacidade entre Fronteiras) e o APEC Privacy Recognition for Processors - PRP (Reconhecimento de Privacidade para Processadores), que foram desenvolvidos pelo fórum da Cooperação Econômica Ásia-Pacífico (APEC) para permitir transferências de dados transfronteiriças.

As APEC Cross Border Privacy Rules para controladores (CBPR) e o APEC Privacy Recognition for Processors (PRP) são códigos de conduta executáveis para transferências de dados transfronteiriças intra e inter-empresariais por empresas que foram avaliadas e certificadas para participação no sistema CBPR por uma organização de certificação de terceiros aprovada e conhecida como um "Agente de Responsabilização".[5] Nesse sentido, têm aplicabilidade mais ampla do que a BCR intra-empresarial na Europa.

Acreditamos que é extremamente importante que a lei de privacidade do Brasil permita sistemas similares ao sistema APEC CBPR para facilitar os fluxos de dados entre o Brasil e a região Ásia-Pacífico e os seus 21 países membros,[6] onde o CBPR provavelmente será o mecanismo de transferência transfronteiriça dominante. Na verdade, a APEC atualmente está considerando permitir que empresas não inclusas na APEC obtenham certificação CBPR, o que abriria a porta

[5] A CBPR para responsáveis acompanha e implementa os nove princípios de privacidade da APEC. A CBPR foi finalizada em 2011 e atualmente está em fase inicial de implementação. Todas as 21 economias membros da APEC aprovaram a CBPR e manifestaram a intenção de aderir ao sistema e reconhecer a CBPR em seu país. Para aderir ao sistema, um país da APEC deve ter pelo menos um órgão de privacidade que possa aplicar a CBPR e um "Agente Responsabilização" que possa certificar organizações. Os atuais participantes são os Estados Unidos, México, Japão e Canadá, e outros países da APEC participarão em breve. Três países latino-americanos (Chile, Peru e México) são membros da APEC e qualificados para participar do sistema CBPR. Em fevereiro de 2015, a APEC aprovou um conjunto resultante de regras de privacidade transfronteiriça para operadores, o PRP (Reconhecimento de Privacidade para Operadores) da APEC. Para saber mais sobre o sistema CBPR, consulte www.cbprs.org.

[6] Estados Unidos; Austrália; Brunei Darussalam; Canadá; Chile; China; Hong Kong, China; Indonésia; Japão; Malásia; México; Nova Zelândia; Papua Nova Guiné; Peru; Filipinas; Rússia; Cingapura; República da Coreia; Taipei chinesa; Tailândia; e Vietnã.

para a participação brasileira direta no sistema. Mesmo sem o sistema CBPR atual estar sendo aberto diretamente para empresas não incluídas na APEC, é importante que as novas leis de privacidade permitam a cooperação e a interoperabilidade entre todos os mecanismos de transferência de dados legítimos. Assim, recomendamos fortemente que o Brasil considere plenamente o sistema APEC CBPR e o que ele implica e inclua mecanismos semelhantes ao APEC CBPR em sua lista de mecanismos de transferência transfronteiriça.

Além disso, recomendamos que a lei inclua um processo pelo qual entidades reconhecidas, que não sejam "órgão público competente", possam analisar e aprovar cláusulas contratuais padrão, regras corporativas globais ou regras de privacidade transfronteiriça semelhantes à APEC CBPR. É provável que qualquer plano de transferência transfronteiriça que se baseie nos recursos de um órgão do governo para aprovação caso a caso venha sob enorme pressão, dada a natureza global da economia da informação e da probabilidade da alta demanda para essa aprovação. Em vez de contar apenas com os órgãos governamentais, recomendamos o modelo APEC de empregar "Agentes de Responsabilização" formalmente reconhecidos para esses fins, de acordo com padrões rigorosos e supervisão.

Também é importante destacar que a responsabilidade conjunta das partes para uma transferência internacional de dados pessoais (cedente e cessionário) é prejudicial para a cadeia de participantes (consulte os Artigos 34(1), 35 e 44). Se o cessionário for um mero processador (ou operador), não é razoável tornar o cessionário responsável pelos atos do titular dos dados, a menos que ele atue fora do escopo requerido pelo cedente. Um ônus excessivo para o cessionário prejudica a cadeia de processadores de dados.

Órgão de proteção de dados/Órgão público competente

Aprovamos a inclusão do Artigo 53 neste anteprojeto, que delineia os deveres específicos de um "órgão público competente". Entendemos, também, que a decisão de não incluir a criação, a definição e as condições deste organismo público competente (ou um órgão de proteção de dados) foi uma escolha política com base nas restrições de orçamento do Poder Executivo. Por outro lado, é nosso entendimento que a iniciativa para a criação de um órgão federal deve vir do Poder Executivo e não pode surgir a partir do debate de um projeto de lei no Poder Legislativo.

A criação de um organismo independente é essencial para estabelecer o melhor sistema de proteção de dados pessoais. Essa entidade poderia ter uma estrutura muito pequena com alcance federal para garantir que as regras e as políticas sejam nacionalmente uniformes. Além disso, garantiria que a adoção dos regulamentos fosse conduzida por funcionários tecnicamente capacitados que atuam de forma independente.

A natureza multidisciplinar da proteção de dados pessoais exige que o órgão de proteção de dados seja independente dos diferentes prismas do governo. Isso garante que abordem o assunto de uma forma equilibrada, incluindo os aspectos de tecnologia e inovação, desenvolvimento local e estrangeiro, a proteção e segurança do consumidor.

Portanto, é altamente recomendável que o anteprojeto de lei preveja a criação, o escopo e os poderes de um órgão de proteção de dados federal, que seja técnico e independente.

Efetividade

Por fim, recomendamos enfaticamente que a lei seja aplicada de forma prospectiva em vez de retroativa.

II. Conclusão

Obrigado por considerar nossas observações e recomendações adicionais. Em caso de dúvidas, entre em contato com Bojana Bellamy, Presidente, Centre for Information Policy Leadership (bbellamy@hunton.com) ou Markus Heyder, VP e Consultor Sênior de Política, Centre for Information Policy Leadership (mheyder@hunton.com).