Centre for Information Policy Leadership
Hunton & Williams LLP

30 ST MARY AXE
LONDON, EC3A 8EP
TEL +44 (0)20 7220 5700
FAX +44 (0)20 7220 5772

2200 PENNSYLVANIA AVENUE NW
WASHINGTON, DC 20037
TEL 202 • 955 • 1500
FAX 202 • 778 • 2201

5 DE MAIO DE 2015

Comentários do Centre for Information Policy Leadership

Anteprojeto de lei do Brasil ("anteprojeto") que dispõe "sobre o tratamento de dados pessoais para proteger a personalidade e a dignidade da pessoa natural"

O Centre for Information Policy Leadership ("Centro") agradece a oportunidade de fornecer comentários sobre o anteprojeto de lei do Brasil que dispõe sobre o tratamento de dados pessoais para proteger a personalidade e a dignidade da pessoa natural". Estabelecido há mais de 12 anos, o Centro é um think tank especializado em segurança e privacidade global do escritório de advocacia, Hunton & Williams. O Centre conta com o apoio de aproximadamente 35 empresas membros que são líderes nos principais setores da economia global. O Centro oferece experiência e liderança sobre problemas de política global de segurança e privacidade, trabalhando 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 saber mais, 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.

I. Declaração geral

O Centro felicita os redatores da lei proposta por terem desenvolvido um anteprojeto que englobe uma ampla gama de proteções fundamentais que precisam estar incluídas em qualquer lei sobre privacidade. O anteprojeto representa um ótimo ponto de partida para desenvolver uma legislação que maximize proteções de privacidade para indivíduos, facilite o uso inovador e benéfico de dados em um ambiente de tecnologia e de negócios em constante mudança e garanta a competitividade econômica do Brasil nesse ambiente.

Apoiamos o reconhecimento do anteprojeto de alguns conceitos de privacidade de dados modernos e melhores práticas. Especificamente, apoiamos o conceito de um órgão nacional e único de proteção de dados ("órgão competente"), a capacidade de obter dados pessoais fora do escopo da lei eliminando a identificação e tornando-os anônimos, o reconhecimento da importância de permitir que dados internacionais entrem e saiam do Brasil através de uma ampla gama de instrumentos e a inclusão do conceito de "boas práticas", que pode ser desenvolvido por organizações para implementar os requisitos da lei e demonstrar conformidade.

Por outro lado, acreditamos que o anteprojeto de lei se beneficiará de determinados esclarecimentos e modificações em algumas áreas. Entre elas, a área de jurisdição, a distinção entre responsáveis e operadores, as especificações do objetivo e o conceito de "compatibilidade",

a natureza de consentimento e as exceções e alternativas adicionais ao consentimento, e as opções de mecanismos de transferências internacionais.

Esperamos que as nossas recomendações abaixo ajudem os redatores na finalização da proposta de uma maneira que cumpra as suas promessas. Nesse sentido, parabenizamos os redatores por iniciarem um processo abrangente de consulta sobre o projeto de lei proposto e consideramos adequado fazer uma segunda rodada de consultas sobre um anteprojeto de lei revisado antes de apresentar o projeto de lei final do órgão executivo para o legislativo. Pela própria natureza, o projeto de lei tem escopo abrangente e afetará todas as áreas de atividade comercial e governamental, pois ele engloba o tratamento de dados pessoais de todos os indivíduos, independentemente de desempenharem o papel de cidadão, funcionário, consumidor, cliente, empresa ou outro papel. Portanto, é essencial que haja uma consulta ampla e solicitação de opiniões, bem como avaliações de impacto de todas as partes interessadas – dos setores públicos e privados, organizações de grande e pequeno porte, incluindo start-ups e todos os setores da indústria e sociedade.

II. Comentários específicos

1. Jurisdição e distinção entre responsável pelo tratamento/operador

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:*
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.

Artigo 6

As atividades de tratamento de dados pessoais deverão atender aos seguintes princípios gerais:

Comentários do Centro: O escopo da jurisdição do anteprojeto parece ser abrangente demais e diferente do que é habitual em outras leis de privacidade de dados em âmbito global. Em algumas partes, também não faz uma distinção clara entre os responsáveis pelo tratamento de dados e operadores de dados (embora sejam tratados separadamente nas definições, Artigo 5 VIII e IX, bem como nos últimos capítulos, incluindo o Capítulo II, Artigos 7, 10 e 11; Capítulo III, Artigo 17 e 19; e Capítulo V, Artigo 30). Tanto a jurisdição abrangente e a falta de uma distinção clara entre as obrigações dos responsáveis e operadores podem criar consequências inesperadas e resultar em interpretações da lei que causam desvantagem comercial para o setor brasileiro de serviços de TI, sem benefícios equivalentes para a proteção de privacidade.

Distinção entre responsável/operador. Em geral, o anteprojeto de lei parece reconhecer que os responsáveis pelo tratamento de dados são as entidades que coletam e usam dados sobre indivíduos para vários fins, são responsáveis por todas as decisões relativas ao tratamento de

dados e podem envolver os operadores de dados de terceiros para executar várias funções de tratamento em seu nome. Dessa forma, parece que o anteprojeto reconhece que os responsáveis são as entidades que devem ser os principais responsáveis pelo cumprimento da legislação de privacidade de dados, pois os operadores de terceiros atuam somente em seu nome e estão meramente implementando qualquer requisito legal de acordo com o contrato e instruções do responsável. Embora a divisão de responsabilidade pareça ser reconhecida em várias partes do anteprojeto de lei, incluindo as definições, essa distinção não está refletida de forma consistente em outras partes do texto, mais destacadamente no Capítulo I, Artigo 2, que define o escopo da lei, e o Artigo 6 que diz respeito aos princípios de tratamento de dados. As duas disposições parecem ser escritas como se aplicassem igualmente aos responsáveis e aos operadores. Isso pode criar incerteza e obrigações conflitantes para os operadores e os responsáveis no Brasil. Sugerimos que a distinção entre os responsáveis e os operadores sejam esclarecidas em toda a lei.

Escopo da jurisdição. No que diz respeito ao escopo da jurisdição do anteprojeto de lei, os responsáveis pelo tratamento de dados estrangeiros não devem estar sujeitos à legislação brasileira sobre privacidade quando usam operadores brasileiros para processar dados que não sejam de brasileiros no Brasil. Exigir a aplicação da lei brasileira de privacidade sobre responsáveis estrangeiros criaria entraves significativos para o setor de serviços de TI do Brasil, bem como para outros operadores no Brasil que prestam serviços a clientes globais.

Além disso, os operadores de dados localizados no Brasil não devem estar sujeitos a lei de privacidade brasileira salvo se por contrato (se eles estiverem fazendo o tratamento de dados em nome dos operadores brasileiros). Na verdade, se eles estiverem processando dados que não sejam de brasileiros em nome de operadores estrangeiros que estão sujeitos às exigências estrangeiras, esses operadores não poderão cumprir as obrigações de privacidade de responsáveis estrangeiros e exigências brasileiras que podem ser conflitantes.

Portanto, na nossa opinião, a jurisdição da lei de privacidade sobre responsáveis deve se estender apenas aos responsáveis estabelecidos no Brasil ou aos responsáveis localizados fora do Brasil, mas que estejam direcionando seus serviços a residentes do Brasil e, propositadamente, coletando dados pessoais de residentes do Brasil (embora, nesse caso, possa ser difícil aplicar a lei se a entidade não tiver presença no Brasil).

Assim, os Artigos 2º e 6º podem ser alterados da seguinte forma:

Artigo 2

A presente Lei ***impõe obrigações sobre*** ~~*aplica-se a operações de tratamento*~~ ***responsáveis com relação às operações de tratamento*** *realizadas por meios totalmente ou parcialmente automatizados* ***direcionadas a indivíduos que residem no Brasil*** ~~*por eles mesmos ou por uma pessoa física ou jurídica nos termos a legislação pública ou civil*~~*, independentemente do país* ***onde os responsáveis*** ~~*se*~~ *se encontram e o país onde* ***ocorre o tratamento*** ~~*a base de dados está localizada*~~*, conquanto que:*
I – ~~*A operação de tratamento seja realizada dentro do território nacional; ou*~~

*~~II –~~ ~~O~~os dados pessoais a serem processados tenham sido **intencionalmente** coletados **de ou sobre indivíduos** no território nacional.*
*§ 1 Os dados pessoais são considerados como coletados **de ou sobre indivíduos** no território nacional se os titulares dos dados estiverem localizados no território nacional no momento da coleta.*

II. Com relação aos requisitos de boas práticas do Art. 48 e 49], esta lei também se aplica aos operadores com operações de tratamento no território nacional.

Artigo 6

***Os responsáveis têm a responsabilidade de garantir que** as atividades de tratamento de dados pessoais deverão atender aos seguintes princípios gerais:*

2. Dados anônimos

Art. 5º Para os fins desta Lei, considera-se:

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;

Comentários do Centro: Esta definição parece não ter aplicação nem consequência *explícita* ao anteprojeto. No entanto, por dedução e em conjunto com as definições de "dados pessoais" e "tratamento" do Artigo 5º, incisos I e II, os dados anônimos não estão sujeitos a essa lei e felicitamos a exceção de dados anônimos nessa lei. Agradecemos também a inclusão no anteprojeto de um componente de razoabilidade e observamos que, embora possa haver circunstâncias criando riscos teóricos de re-identificação, em muitos casos, esses riscos teóricos são remotos e a privacidade dos brasileiros é mais bem atendida por incentivar as organizações a retirar a identificação de dados pessoais. No entanto, recomendamos que o objetivo desta disposição seja explicitado, afirmando claramente que a retirada de identificação e anonimato de dados pessoais afasta esses dados do âmbito dessa lei. Por exemplo, dados anônimos devem ser explicitamente excluídos da definição de "dados pessoais" no Artigo 5 I.

3. Princípios, especificação de finalidade e "Compatibilidade"

***Art. 6º** As atividades de tratamento de dados pessoais deverão atender aos seguintes princípios gerais:*

I – princípio da finalidade, pelo qual o tratamento deve ser realizado com finalidades legítimas, específicas, explícitas e conhecidas pelo titular;

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;

Comentários do Centro: Com relação ao primeiro princípio, sugerimos expandir o alcance de "conhecidas pelo titular" para incluir o que é esperado pelo titular de dados em virtude do contexto do tratamento.

Além disso, apoiamos o segundo princípio até o limite em que dispõe que o tratamento é permitido desde que possa ocorrer e coexistir sem conflito com a finalidade inicial ou expectativas do titular de dados (*isto é,* seja "compatível" com a finalidade inicial e as expectativas). Este é exatamente o caso de muitos novos usos benéficos e adicionais de dados em que esses usos ainda não são conhecidos ou conhecíveis no momento da coleta, mas em que esses novos usos não prejudiquem a finalidade original e possam coexistir com ela.

Por exemplo, muitos aplicativos de Big Data e analíticos oferecem benefícios tangíveis a indivíduos e à sociedade como um todo, possibilitando pesquisa médica mais orientada, fornecendo melhor assistência médica, permitindo uso mais eficiente de serviços públicos e recursos e na prevensão de fraudes.

- Big data e analíticos vêm transformando o setor de assistência médica, pois correlacionam dados de pacientes de uma ampla gama de fontes e revelam padrões que podem, por exemplo, identificar indivíduos com maior probabilidade de usar serviços de emergência. Quando o Dr. Jeffrey Brenner reuniu registros de 600.000 consultas hospitalares em Camden, NJ, ele não tinha certeza do que descobriria. Ele criou um mapa ligando processos hospitalares ao endereço dos pacientes e para sua surpresa, apenas 1% dos pacientes eram responsáveis por 30% das contas do hospital. Esses pacientes estavam comparecendo a consultas hospitalares com muita frequência, acarretando custos significativos ao sistema de assistência médica. Fornecer assistência mais eficiente e eficaz a esses tipos de paciente é um desafio enfrentado pelo sistema de assistência médica no mundo todo. Contudo, usando o poder dos dados nesse caso específico, assistentes sociais conseguiram identificar pacientes específicos e fazer consultas domiciliares proativas para incentivar esses pacientes de alto risco a continuarem tomando a medicação. Isso resultou em uma redução surpreendente nas contas hospitalares naquela região.

- O New York Police Department (NYPD) tem usado cada vez mais tecnologia de big data para combater crimes. O Domain Awareness System do NYPD, criado em 2012, contém todos os dados de registros de prisão, portes de arma, mandados de prisão pendentes até textos de ligações feitas ao 911 em tempo real. Isso permite que policiais acessem informações cruciais antes de responder a um crime. O sistema é tão eficiente que o NYPD está desenvolvendo um aplicativo para tablets e telefones, para que os policiais possam acessar as informações quando estiverem em trânsito.

- O Big Data vem sendo usado para detectar fraudes em declarações de imposto de renda. Um relatório da procuradoria geral de administração tributária do Tesouro Norte-Americano estimou que as fraudes de devoluções de impostos resultantes de roubo de identidade totalizaram aproximadamente US$ 3,6 bilhões durante o período de entrega das declarações de 2011. Esse número caiu para US$ 1,6 bilhão desde o ano anterior graças ao uso de ferramentas de Big Data para melhor detectar essas declarações de

impostos fraudulentas. Essas ferramentas fazem a varredura de vários bancos de dados de informações públicas para encontrar declarações fraudulentas.

Para que haja crescimento econômico, a oferta de novos produtos e serviços e outros benefícios públicos baseados em inovação orientada por dados, é importante que o sistema jurídico seja flexível o bastante para permitir novas finalidades e usos de dados e, ao mesmo tempo, proteja os direitos de privacidade dos indivíduos.

No entanto, para garantir a correta interpretação do que é uma finalidade compatível, é recomendável incluir algumas orientações adicionais sobre os fatores que os responsáveis devem levar em conta ao determinar se uma finalidade posterior é compatível ou não. Este é o tratamento adotado na Europa pelo Grupo de Trabalho do Artigo 29[1] em seu parecer de abril de 2014 sobre o limite da finalidade (Parecer 03/2013 sobre o limite da finalidade, 00569/13/EN WP 203), bem como nas discussões no Conselho Europeu sobre a proposta Regulação de Proteção de Dados da UE. Por exemplo, de acordo com o Grupo de Trabalho do Artigo 29, o teste de "incompatibilidade" inclui uma avaliação dos impactos negativos e positivos do tratamento adicional proposto sobre o titular de dados, pelo qual quanto mais negativo ou incerto for o impacto, menor será probabilidade de o tratamento ser considerado "compatível."

Por fim, quando o teste pertinente determinar a "incompatibilidade", deve existir, não obstante, a capacidade de processar dados quando houver um "interesse legítimo" em assim fazê-lo. (*Leia* a discussão sobre o motivo de "interesse legítimo" para tratamento na Seção 4 relacionada a "consentimento" que se encontra abaixo.)

Assim, gostaríamos de fazer as seguintes recomendações quanto aos princípios I e II:

As atividades de tratamento de dados pessoais deverão atender aos seguintes princípios gerais:

I – Princípio de finalidade, pelo qual o tratamento deve ser realizado para finalidades legítimas, específicas e explícitas que sejam conhecidas, ***ou razoavelmente esperadas,*** *pelo titular;* ***considerando o contexto do tratamento****;*

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;

Ao decidir se um tratamento posterior é compatível com as finalidades originais , o responsável deve considerar
a) qualquer vínculo entre os propósitos originais buscados e os efeitos de tratamento adicional pretendido;
b) o contexto no qual os dados foram coletados e processados;

[1] O Grupo de Trabalho do Artigo 29 inclui os líderes de todos os órgãos de proteção de dados da UE. Entre outros aspectos, este grupo elabora interpretações escritas e pareceres sobre os princípios e exigências contidas na Diretiva de Proteção de Dados da UE atual, incluindo vários que são relevantes para comentários do Centro, como os conceitos de limitações de finalidade, interesse legítimo, responsabilização e o conceito de "Regras Empresariais Obrigatórias." Mais informações sobre o Grupo de Trabalho do Artigo 29 estão disponíveis em http://ec.europa.eu/justice/data-protection/article-29/index_en.htm.

c) a natureza dos dados pessoais;
d) qualquer impacto do tratamento adicional sobre o titular de dados, inclusive a probabilidade e gravidade de danos aos titulares de dados; e
e) a existência de proteções apropriadas

Quando a finalidade de tratamento adicional não for compatível com as finalidades originais procuradas e com as expectativas legítimas do titular de dados, conforme o contexto do tratamento, o tratamento adicional precisa seguir o Capítulo II, Seção I, quanto ao consentimento e exceções ao consentimento. O tratamento adicional para finalidades incompatíveis com base em interesses legítimos do responsável ou de um terceiro será lícito, se tais interesses substituírem os interesses do titular de dados.

4. 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.*

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

Comentários do Centro: O consentimento é uma base importante para o tratamento de dados, porém, nem todo tratamento de dados pode ou deve ter por base o consentimento. Em especial, a dependência excessiva no consentimento pode resultar em fadiga do consumidor, apatia e perda da capacidade de distinguir entre tratamento e coleta de dados, criando riscos significativos de privacidade provenientes das atividades que não o seguem. Alguns contextos exigem alternativas ao consentimento que ainda não foram incluídas nas exceções previstas no anteprojeto de lei. Além disso, nem todo consentimento deve ser expresso, desde que seja livre, específico e informado.

Em alguns contextos, os responsáveis podem processar dados com base em outros critérios, por exemplo, onde existe um "interesse legítimo" no tratamento. "Interesse legítimo" é um dos pilares para tratamento nos termos da Diretiva de Proteção de Dados da União Europeia e da proposta Regulação de Proteção de Dados da UE. Permite que um responsável processe os dados, se for necessário para um interesse legítimo do responsável ou de um terceiro que não seja menos importante que os direitos ou liberdades fundamentais do titular de dados. De acordo com o parecer de abril de 2014 do Grupo de Trabalho do Artigo 29 sobre "interesse legítimo" (Parecer 06/2014 sobre a noção de interesse legítimo do responsável pelo tratamento de dados nos termos do Artigo 7º da Diretiva 95/46/EC, 844/14/EN, WP 217), a análise da possibilidade de o motivo de interesse legítimo poder ser atendido envolve análise de riscos/benefícios contextuais, específicos por caso comparando o interesse do responsável com os danos potenciais para o titular de dados. (*Leia também* abaixo a discussão sobre avaliações de risco e gestão de risco de privacidade na Seção 7 sobre "Boas Práticas".)

Uma exceção para interesse legítimo para o tratamento é importante principalmente no contexto do aumento de digitalização de processos comerciais e da sociedade e em conexão com a Internet das Coisas e análise de big data, em que o consentimento expresso e específico nem

sempre pode ser obtido na prática. Nesses casos, deve haver outros motivos legítimos de tratamento para facilitar os usos de dados de forma responsável e transparente, que sejam benéficos para os indivíduos e para a sociedade e que permitam práticas comerciais legítimas e inovação, evitando danos e respeitando a privacidade dos indivíduos. A aplicação rígida de uma exigência de consentimento em casos que seria impraticável ou inadequado obter o consentimento válido, resultaria em consentimentos ilusórios, desinformados e sem sentido, prejudicando a eficaz proteção de privacidade. Assim, para garantir que as regras de privacidade de dados permaneçam tecnologicamente neutras e possam ser aplicadas contextualmente no futuro, é necessário fornecer motivos adicionais e mais flexíveis para o tratamento, como interesse legítimo (além das outras exceções ao consentimento previsto no anteprojeto).

Além disso, as organizações têm o direito e uma necessidade crescente de proteger seus dados, propriedade intelectual, redes e sistemas de TI e outros ativos contra usos fraudulentos ou ataques de cibersegurança. Essas medidas de proteção muitas vezes exigem o tratamento de dados pessoais de indivíduos, inclusive aqueles que possam estar envolvidos em atividade fraudulenta ou ataques de cibersegurança. Obter consentimento nessas circunstâncias anula a finalidade do tratamento. Acreditamos que estes exemplos de tratamento também devem se basear em uma exceção de “interesse legítimo.”

Outros exemplos de tratamento baseados em interesse legítimo incluem o uso de dados por organizações para comercializar os próprios produtos e serviços, bem como o uso comercial de dados dentro de uma organização para melhorar seus produtos e serviços e para permitir a colaboração e o compartilhamento de informações dentro da organização para essas finalidades.

O consentimento também não deve ser obrigatório quando o tratamento for necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados. Essa exceção também está incluída na Diretiva de Proteção de Dados da UE e está alinhada à Lei de Acesso à Informação do Brasil (Lei nº 12.527de 18 de novembro de 2011), que elimina a necessidade de consentimento em diversas circunstâncias, inclusive "à proteção do interesse público e geral preponderante” (Artigo 31, V). Uma exceção no caso de interesse público é importante para as autoridades tributárias conseguirem coletar e processar a declaração de imposto de renda de um indivíduo para determinar e confirmar a quantidade de impostos a ser paga. Outro exemplo é uma associação médica profissional que é responsável por realizar procedimentos disciplinares contra membros no caso de fraude e abuso médico. Todos esses casos são de interesse público, em que um indivíduo, como o médico que cometeu a fraude, não consentiria com a inclusão de informações pessoais em um banco de dados, se ele tivesse essa opção. Casos como os mencionados são benéficos à sociedade e devem ser reconhecidos no Anteprojeto como já está previsto na Lei de Acesso à Informação.

Por fim, exigir que consentimento seja “expresso” em todos os casos também sugere que o “opt-out” não seria uma opção. No entanto, em alguns contextos, o opt-out pode ser uma opção mais adequada. Assim, seria bom permitir maior flexibilidade na definição de consentimento e não especificar o tipo de consentimento necessário.

Em suma, do ponto de vista de políticas públicas, o excesso de dependência de consentimento, na verdade, não protege os indivíduos. A experiência comprova que a maioria dos indivíduos não lê nem compreende as longas e complicadas políticas e avisos de privacidade. Consequentemente, não representam uma base eficaz de escolha e controle do indivíduo e, na verdade, qualquer "consentimento" baseado nesses avisos é ilusório. Um exemplo disso é a exigência, na Europa, de obtenção de consentimento expresso para o uso de cookies e qualquer tecnologia de rastreamento de hard drives de um indivíduo. Resultou em uma avalanche de avisos sem sentido sobre cookies em websites europeus que o usuário, em vez de realmente ler, simplesmente clica para que esses avisos desapareçam. Obviamente, o processo de consentimento não está funcionando nesse contexto.

Dessa forma, recomendamos os seguintes acréscimos às exceções ao consentimento nos Artigos 7º e 11:

Art. 7º – O tratamento de dados pessoais somente é permitido quando o consentimento livre, ~~expresso~~, específico e informado é dado pelo titular de dados, salvo no caso contemplado no Artigo 11.

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

VIII – processar os dados de forma compatível com um interesse legítimo do responsável ou de um terceiro, desde que esses interesses não sejam anulados por danos ou impacto negativo sobre o titular de dados.

IX - O tratamento for necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados

5. Transferências internacionais

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:*
...
III – quando órgão competente autorizar a transferência, nos termos de regulamento;

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.*

§ 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.

§ 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.

Comentários do Centro: O Centro acolhe com prazer o enfoque do anteprojeto de lei para transferências de dados internacionais até o limite em que disponha sobre um espectro de mecanismos que possam ser usados para legitimar transferências de dados pessoais para países que não tenham níveis similares de proteção de dados.

Acolhemos a incorporação de conceitos de ampla aceitação de "cláusulas contratuais padrão" e "normas societárias globais" ou "regras societárias globais" (conhecidas na Europa como "Regras Empresariais Obrigatórias", BCR[2]). Estes conceitos são bons pontos de partida para posicionar o Brasil para transferências de dados com a Europa e outros países que reconhecem esses mecanismos europeus de transferências internacionais. No entanto, as cláusulas contratuais padrão e regras empresariais obrigatórias têm suas limitações – as primeiras podem resultar em uma complexidade desnecessária e as últimas estão limitadas a transferências dentro de um grupo de empresas e sem escalabilidade. Por isso, ao mesmo tempo em que incentivamos o Brasil a incluir essas opções como mecanismos legítimos para transferências internacionais de dados, também incentivamos o Brasil a trabalhar com especialistas experientes nesses mecanismos, incluindo o Centre, para melhorar e torná-los mais práticos e escalonáveispara uso mais amplo por empresas de todos os portes.

Além disso, visto que os fluxos de dados modernos e atividade econômica são verdadeiramente globais por natureza, é importante incluir no menu de opções um mecanismo adicional de transferência internacional que reflita aqueles que estão disponíveis em outras jurisdições e regiões e que vãoalém de transferências intraempresas. Assim, incentivamos a inclusão de mecanismos adicionais, como marcas e selos de privacidade e outros códigos de conduta organizacional que são certificados por terceiros apropriados ou um órgão competente.

Um exemplo é o sistema de Regras de Privacidade Transfronteiriças da APEC desenvolvido pelo Fórum de Cooperação Econômica Ásia-Pacífico (APEC). As Regras de Privacidade Transfronteiriças (CBPR) para responsáveis da APEC e as Regras de Privacidade para Operadores (PRP) da APEC são códigos de conduta aplicáveis para transferências internacionais de dados intra e entre empresas, que foram analisadas e certificadas para participação no sistema

[2] As Regras Empresariais Obrigatórias da UE (inclusive regras do responsável e do operador) são normas internas legalmente aplicáveis dentro de uma família corporativa para o tratamento de dados pessoais que, mediante aprovação do órgão de proteção de dados, são um mecanismo de transferência transfronteiriça nos termos da Diretiva de Proteção de Dados da UE atual.

de CBPR por uma organização certificadora externa e aprovada conhecida como "Agente de Responsabilização." A aplicação da CBPR é feita pelos órgãos de proteção de dados da APEC e de privacidade de participantes que assinaram o Acordo de Execução de Privacidade Transfronteiriças (CPEA) da APEC.[3]

Ressaltamos que os mecanismos de transferência de dados devem permitir as transferências não apenas dentro de um grupo empresarial global que implementou e aprovou suas regras empresariais globais, mas também entre empresas não associadas, como é o caso atual da CBPR da APEC e, provavelmente, passe a ser caso com a BCR na Europa, conforme o proposto Regulamento de Proteção de Dados da UE.

No que diz respeito à exigência no anteprojeto atual de que o "órgão competente" autorize esses padrões empresariais globais, recomendamos que essa exigência seja modificada para reconhecer as autorizações dessas regras empresariais pelos órgãos estrangeiros competentes, no que diz respeito às normas empresariais globais e qualquer sistema de código de conduta ou sistema de regras de privacidade transfronteiriça semelhante à CBPR da APEC. Exigir que as organizações busquem aprovação ou autorização para suas regras empresariais de vários órgãos e várias jurisdições ocasionaria ineficiências significativas, comprometeria a utilidade e eficácia desses mecanismos de transferências transfronteiriças e impediria a expansão eficaz para as PMEs. Isso é evidenciado pela experiência europeia com o BCR, que resultou na possibilidade de agora obter a autorização de um órgão "líder" na Europa, em um processo de reconhecimento mútuo. Essa é também a razão pela qual a CBPR da APEC exige certificação de acordo com a CBPR em apenas um país da APEC em que a empresa ou grupo de empresas esteja sediada.

Na verdade, um trabalho está sendo realizado entre a APEC e o Grupo de Trabalho do Artigo 29 da UE para explorar maneiras de otimização da certificação CBPR/BCR e processos de aprovação nos quais as empresas busquem "certificação dupla" para os dois sistemas. Assim, o Centre recomenda que as eventuais contrapartidas brasileiras a esses mecanismos sejam concebidas para que sejam "interoperáveis" com outros esquemas de transferência internacionais semelhantes, para garantir que as empresas que tenham certificado ou sejam aprovadas por um regime não brasileiro possam ser consideradas autorizadas no Brasil até o limite em que houver sobreposição de requisitos e *vice-versa*.

Além disso, em virtude da necessidade cada vez maior de transferências internacionais de dados, para evitar sobrecarregar qualquer futuro órgão de proteção de dados brasileiros, o anteprojeto deve incluir uma cláusula que permita o uso de cláusulas contratuais padrão pré-autorizadas,

[3] 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 pode aplicar a CBPR e um "Agente Responsabilização" que pode certificar organizações. Os participantes atuais são EUA, México e Japão. O Canadá está prestes a fazer parte formalmente e, em breve, outros países da APEC seguirão o exemplo. 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.

tanto para transferências para os responsáveis quanto para transferências para operadores (semelhantes às da UE).

Finalmente, além de transferências de dados que estão sujeitas à autorização do órgão de proteção de dados no Art. 28 e aquelas que estão sujeitas a consentimento no Art. 29, deve haver uma disposição para permitir as transferências de dados pessoais em casos semelhantes às exceções para consentimento no Art. 11 do anteprojeto. Assim, as transferências de dados para países terceiros devem ser permitidas com as mesmas exceções que existem com relação ao consentimento para tratamento de dados no Brasil. Isso é compatível com outras leis de privacidade que também contêm restrições às transferências internacionais de dados.

Dessa forma, recomendamos as seguintes alterações para os seguintes artigos:

Artigo 28

A transferência internacional de dados pessoais somente é permitida para países que proporcionem nível de proteção de dados pessoais equiparável ao dessa Lei, ressalvadas as seguintes exceções:

. . .

VI. – (nova disposição) Quando a transferência ocorrer em uma das condições para a qual não é necessária autorização nos termos do Artigo 11.

Artigo 30 – (referente à Autorização no Art. 28 Seção III)

A autorização referida no inciso III do caput do Artigo 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.

§ 1º O Órgão competente poderá elaborar cláusulas contratuais-padrão ***para transferências de responsável pelo tratamento para responsável pelo tratamento e de responsável pelo tratamento para operador****, que deverão observar os princípios gerais de proteção de dados e os direitos do titular, garantida a responsabilidade solidária, independentemente de culpa, de cedente e cessionário.* ***O uso de cláusulas contratuais padrão não estará sujeito à autorização individual mencionada na Seção II do caput do Artigo 28.***

§ 2 Os operadores e responsáveis, ou grupos de operadores e responsáveis, ~~que sejam parte de um mesmo grupo econômico ou conglomerado multinacional~~ podem enviar regras empresariais globais ***aplicáveis*** *para aprovação pelo órgão competente* ***ou regras empresariais globais que tenham sido aprovadas por um órgão competente estrangeiro****,* ***ou podem apresentar comprovação de participação em um código de conduta transfronteiriça aplicável ou um selo ou marca de privacidade,*** *~~que será obrigatório para todas as empresas~~ ~~no grupo ou~~*

~~*conglomerado*~~ *sem necessidade de autorizações -específicas* ***até o limite em que esses instrumentos cumpram,*** ~~*sujeito à adesão,*~~ *os princípios gerais de proteção e os direitos do titular de dados.*

6. Dados transferidos para o Brasil e consentimento

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.*

Comentários do Centro: Muitas jurisdições (se não a maioria) não requerem consentimento ou contam com bases alternativas ou exceções de consentimento para o uso de dados (*por exemplo,* o interesse legítimo da UE ou as exceções para consentir em Cingapura). Assim, qualquer exigência de que os dados transferidos para o Brasil para tratamento estejam sujeitos às exigências brasileiras de consentimento na jurisdição estrangeira excluirá dados da maioria das jurisdições e prejudicará sobremaneira a capacidade de tratamento de dados estrangeiros pelas empresas brasileiras. Na verdade, essa disposição impediria os responsáveis estrangeiros por tratamento de usar operadores brasileiros localizados no Brasil e, assim, comprometer o crescente setor de serviços de TI no Brasil. Recomendamos a retirada dessa exigência.

7. 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 [sic], poderão ser reconhecidas e divulgadas pelo órgão competente.

Comentários do Centro: O Centro acolhe essa disposição, que parece aceitar os modernos conceitos de responsabilização organizacional (programas de privacidade da empresa) e os códigos de conduta organizacionais ou setoriais. No entanto, recomendamos cinco áreas em que o conceito de "boas práticas" poderia ser esclarecido e elaborado mais.

Em primeiro lugar, para garantir a coerência global, essa disposição pode esclarecer que essas "regras de boas práticas" abrangeriam todo o leque de elementos essenciais da "responsabilização organizacional", pois estão sendo reconhecidas progressivamente em outras diretrizes internacionais, no que diz respeito à responsabilização, e discutidas no trabalho do Centre. Isso incluiria supervisão e verificação interna, avaliação de risco, políticas e procedimentos internos, treinamento, aplicação interna e tratamento de reclamações. Para saber mais sobre os elementos essenciais e tipos de responsabilização, *consulte* http://www.huntonfiles.com/files/webupload/CIPL_Centre_Accountability_Data_Governance_Paper_2011.pdf.

Em segundo lugar, recomendamos que qualquer disposição sobre boas práticas de gestão de risco enfatize expressamente a privacidade como parte integrante da responsabilização da organização e como instrumento necessário para a implementação e ajuste efetivo das exigências legais aplicáveis, com base em contexto e nos riscos de privacidade reais existentes.

De fato, os mecanismos de avaliação de risco que são capazes de avaliar os riscos *e* benefícios para indivíduos do tratamento de dados propostos são cada vez mais importantes na era moderna da informação, não apenas no contexto de big data, Internet das Coisas e tratamento de dados não baseado necessarimanete em consentimento, como em relação a "interesse legítimo" e para os fins de determinação de "compatibilidade" de novos usos de dados adicionais (*consulte* Seções 3 e 4 acima), mas também com relação a praticamente todo o tratamento de dados. Os principais benefícios de um enfoque de gestão de risco para o tratamento de dados incluem o seguinte:

- A avaliação de risco de privacidade ajuda organizações a determinar se e como proceder com os usos de informação propostos com base em uma melhor compreensão de riscos e danos reais ou potenciais que podem causar aos indivíduos. Especificamente, a compreensão da probabilidade e possibilidade de gravidade de danos aos indivíduos, que podem resultar de usos propostos de informações em contextos específicos, permite que as organizações elaborem mitigações e controles adequados e mais específicos e também facilita equilibrar benefícios equivalentes do uso proposto contra qualquer risco residual de danos após a implementação de mitigações antes de tomar qualquer decisão com relação a esse uso.

- As avaliações de risco de privacidade colocam o ônus da proteção da privacidade na organização e são especialmente úteis em situações em que o controle individual e consentimento seriam impossíveis ou onerosos devido à ausência de interação direta com o indivíduo ou à complexidade do tratamento de informações pertinentes, como acontece com frequência cada vez maior.

- As avaliações de risco de privacidade também reduzem a implantação ineficiente dos recursos organizacionais, permitindo que as empresas priorizem seus controles de privacidade de acordo com a probabilidade e gravidade de danos associados ao uso proposto dos dados. É provável que essa priorização contribua para a eficácia geral das proteções de privacidade.

Assim, para tornar-se uma lei de privacidade verdadeiramente eficaz, como resultado das exigências da era moderna de informação, o anteprojeto de lei deve ser sensível ao fato de que diferentes tipos de dados e diferentes tipos de usos podem apresentar diferentes níveis de risco e, portanto, exigem respostas de conformidade sutis "baseadas em risco". Dessa forma, a avaliação de riscos de privacidade e gerenciamento de riscos de privacidade devem ser integrados de forma mais proeminente no anteprojeto de lei em locais apropriados, inclusive, entre outros, a seção de "boas práticas". Para saber mais sobre o papel da gestão de risco no contexto da proteção à privacidade e das estruturas de boas práticas recomendadas, consulte dois *white papers* do Centre sobre o tema: "A Risk-based Approach to Privacy: Improving Effectiveness in Practice", disponível em

http://www.informationpolicycentre.com/files/Uploads/Documents/Centre/A_Risk-based_Approach_to_Privacy_Improving_Effectiveness_in_Practice.pdf e "The Role of Risk Management in Data Protection", disponível em http://www.informationpolicycentre.com/files/Uploads/Documents/Centre/The_Role_of_Risk_Management_in_Data_Protection_FINAL_Paper.PDF.

Em terceiro lugar, a disposição deve também estabelecer incentivos e vantagens para as empresas formularem ou participarem dessas regras de boas práticas. Por exemplo, empresas que participam dessas regras e são capazes de demonstrar esforços de boa-fé de conformidade em um processo de aplicação, podem receber penalidade menor em caso de infração, de acordo com o Capítulo VIII referente a "Penalidades Administrativas".

Em quarto lugar, a disposição deve esclarecer que essas "regras de boas práticas" podem também servir como mecanismos reconhecidos de transferência internacional, como descrito acima na Seção 5 sobre transferências internacionais de dados.

Em quinto lugar, é necessário ressaltar que as regras de boas práticas se aplicam a responsáveis e operadores, já que ambos beneficiariam-se da implementação de programas proativos de privacidade e gestão de segurança.

Por meio de uma alteração textual específica para incorporar uma abordagem baseada em risco para conformidade, recomendamos o seguinte texto:

Novo Artigo ___:

Ao estabelecer regras de boas práticas, o responsável pelo tratamento e o operador 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.

8. Prazo para adoção

Art. 52. *Esta Lei entrará em vigor no prazo de 120 (cento e vinte) dias contados da data da sua publicação.*

Comentários do Centro: Insistimos que o prazo seja prolongado significativamente para que as empresas possam adotar a nova lei. Um prazo razoável seria de pelo menos um ano.

9. Órgão competente

Comentários do Centro: Muitas disposições do anteprojeto de lei não podem ser implementadas sem o "órgão competente" mencionado ao longo do texto, porém o anteprojeto de lei não trata da criação desse órgão. A experiência com outras leis de privacidade e fiscalização de dados no mundo demonstra que para essa lei ser eficaz, um único órgão independente para proteção de dados e aplicação de privacidade ("órgão competente") é essencial e deve ser criado simultaneamente ao anteprojeto de lei. Para garantir a coerência na interpretação e aplicação da

lei, é importante que haja um único órgão nacional competente, em vez de vários órgãos competentes. [4]

Os órgãos nacionais de controle à proteção de dados e órgãos responsáveis pela imposição da privacidade desempenham um papel importante na supervisão, aplicação, interpretação, educação e cumprimento da lei nacional de proteção à privacidade de dados. Muito mais do que tribunais, os órgãos nacionais têm a experiência necessária para interpretar a lei de privacidade com a nuance e a flexibilidade adequada às circunstâncias. Esses órgãos também desempenham o importante papel de ouvidoria para resolver queixas de indivíduos. Finalmente, é importante ressaltar que esses órgãos são indispensáveis para garantir uma abordagem mais harmônica e consistente com a regulamentação e o cumprimento da lei de proteção à privacidade de dados entre países. Os órgãos nacionais de cumprimento da lei de privacidade e proteção de dados trabalham em conjunto por meio de organizações internacionais e regionais como International Conference of Data Protection and Privacy Commissioners, [5] Asia Pacific Privacy Authorities (APPA), [6]Ibero-American Data Protection Network (RIPD), APEC Cross-border Privacy Enforcement Arrangement (CPEA) [7] e Global Privacy Enforcement Network (GPEN). [8] É de importância vital que o Brasil seja representado nessas organizações por meio de um órgão nacional de proteção à privacidade.

III. Conclusão

Obrigado por considerar nossas observações e recomendações. Em caso de dúvidas ou se precisar de mais informações, 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).

[4] A maioria das leis de proteção a dados dispõem sobre um único órgão de proteção de dados. Até mesmo o Japão, que dispôs sobre os vários Ministérios supervisionarem e fiscalizarem o cumprimento da lei de proteção de dados japonesa nas respectivas áreas de responsabilidade, está revisando sua lei para dispor sobre um único órgão de proteção de dados. *Consulte Outline of the System Reform Concerning the Utilization of Personal Data,* Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society (IT Strategic Headquarters), 24 de junho de 2014, disponível em http://kipis.sfc.keio.ac.jp/wp-content/uploads/2014/07/English-Translation-of-Japanese-Government-Proposal-on-Privacy.pdf.

[5] http://icdppc.org/

[6] http://www.appaforum.org/

[7] https://www.privacyenforcement.net/

[8] https://www.privacyenforcement.net/