Coletânea de Trechos dos Comentários do Anteprojeto de Privacidade do Ministério da Justiça de 16 de maio de 2016 e da Carta ao Senador Aloysio Nunes sobre PLS 330/2013:

A seguir são trechos dos comentários formais do Centre for Information Policy Leadership (CIPL) sobre o anteprojeto de privacidade do Ministério da Justiça, relative tanto a versão inicial de janeiro de 2015 e da versão revista de outubro de 2015. Estes comentários são relevantes para comparar disposições do Projeto de Lei do Senado 330 de 2013.

1. 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.

2. 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 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.[1]

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.

[1] 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.

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.

3. 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.

4. Transferências internacionais

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 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]

[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.

[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

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.

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, 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.

"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.