U.S. CHAMBER OF COMMERCE

U.S. Chamber of Commerce comenta as emendas ao Projeto de Lei 4060/2012 da Câmara dos Deputados

The U.S. Chamber of Commerce ("Câmara de Comércio") é a maior federação de negócios do mundo, representando os interesses de mais de três milhões de empresas e organizações de todas as dimensões, setores e regiões, incluindo membros que oferecem empregos para milhares de cidadãos brasileiros. Somos firmes partidários de um produtivo relacionamento entre EUA e Brasil, e nossos membros são representantes de uma comunidade empresarial vital que contribui substancialmente para o aumento do emprego e do crescimento tanto no Brasil quanto nos Estados Unidos.

Ficamos honrados com a oportunidade de comentar a versão mais recente do projeto de lei 4060/2012 da Câmara dos Deputados. A Câmara de Comércio apoia o desenvolvimento de regimes de privacidade de dados claros e consistentes que protejam os consumidores e promovam a inovação por meio da movimentação de dados. Listamos abaixo algumas sugestões para o projeto de lei para ajudar que este atinja esses objetivos. Colocamo-nos à disposição para auxiliar no desenvolvimento de regulamentos que garantam a proteção da privacidade do público por meio do aprimoramento do regime de privacidade de dados de forma eficiente, flexível, prática e que permita o desenvolvimento inovador contínuo que mantenha e crie benefícios a consumidores, reguladoras e empresas.

Em geral, congratulamo-nos com as melhoras feitas no projeto atual sobre as versões anteriores. Sugerimos que o projeto de lei priorize a movimentação dos dados. Também incentivamos melhorar as práticas internacionais existentes, como as encontradas na Organização de Cooperação e Desenvolvimento Econômico (OECD)[1] E Cooperação Econômica Ásia-Pacífico[2] como um guia para o desenvolvimento da regulamentação do comércio eletrônico e das interações na economia digital. Acreditamos que a capacidade de movimentar dados por meio das fronteiras pode coexistir com fortes regras de proteção de dados. Uma estrutura de transferência de dados que facilite os fluxos de dados entre fronteiras permitirá que empresas brasileiras de todos os setores e tamanhos cheguem a novos clientes em mercados estrangeiros de forma barata e gerenciem relacionamentos com clientes estrangeiros.

Além das melhoras já feitas ao projeto, apresentamos comentários pormenorizados que podem ajudar a aprimorar o texto.

Escopo da Lei

Acreditamos que qualquer lei de proteção de dados não deve ter um escopo muito amplo. A linguagem do projeto de lei atual cria incerteza para as empresas. Ele sugere que as empresas não estabelecidas no Brasil podem estar sujeitas à futura lei que poderia impedi-las de oferecer

[1] Veja http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm para "Orientações da OCDE sobre a Proteção da Privacidade e Fluxos entre fronteiras de Dados Pessoais."
[2] Veja http://www.cbprs.org/ Para obter mais informações sobre o regulamento de privacidade entre fronteiras da APEC.

serviços no Brasil, diminuindo assim o investimento estrangeiro no Brasil. Além disso, o amplo escopo do projeto de lei sugere que a lei brasileira se aplica ao processamento de dados pessoais de estrangeiros no Brasil. Tal disposição poderia desencorajar as empresas de estabelecerem seus negócios no Brasil. Por exemplo, uma empresa pode evitar a construção de um *data center* no Brasil, uma vez que a empresa seria obrigada a cumprir a legislação brasileira, mesmo que o *data center* não processasse dados pessoais de brasileiros. Além disso, as empresas internacionais podem evitar fazer negócios com brasileiros por questões de compliance. Isso prejudicaria a capacidade do Brasil de participar de um mercado global, além de limitar as opções para os brasileiros e diminuir o acesso a bens e serviços digitais.

O escopo do projeto de lei atual poderá dificultar no Brasil um ambiente amigável para a exportação de serviços de dados. Portanto, sugerimos ajustar o artigo 3 do projeto de lei para estabelecer que os processadores de dados no Brasil precisem apenas coletar e processar dados pessoais de cidadãos brasileiros.

Definições de Dados

Dados pessoais

A Câmara de Comércio entende que a definição de dados pessoais proposta pelo projeto pode ser menos ampla, enquadrando menos informações gerais como dados pessoais. A definição de dados pessoais não deveria incluir informação que não tenha ligação imediata com um indivíduo específico. Em particular, a utilização da expressão "relacionada com" poderia ser retirada do texto, já que ela se refere a informações que não podem ser utilizadas para identificar especificamente um indivíduo.

O projeto de lei poderia, como sugestão, manter a definição de dados pessoais aos tipos de dados que permitem a identificação de uma pessoa específica. Qualquer definição que seja excessivamente ampla ou crie incerteza poderia ser evitada. Um conceito de dados pessoais amplo e incerto poderia pôr em risco a inovação e o desenvolvimento econômico baseados na utilização e transferência de dados.

Dados sensíveis

Apesar de apoiarmos a criação de diferentes categorias de dados a fim de facilitar uma abordagem de proteção de dados baseada no risco, alguns dos termos desta definição são pouco claros. Primeiramente, sugerimos a retirada do texto da expressão "crenças filosóficas" porque o tipo de dados que se enquadram nesta categoria é muitas vezes bastante subjetivo. Em segundo lugar, sugerimos refinar ainda mais o que se entende por dados de "saúde". Por exemplo, deve haver uma diferença entre dados confidenciais relacionados a um exame médico em comparação com a frequência cardíaca gravada em um aplicativo enquanto uma pessoa faz exercícios físicos. Os produtos de consumo e aplicativos móveis de saúde estão preparados para um crescimento exponencial e queremos garantir que os cidadãos brasileiros tenham acesso a essa tecnologia de ponta.

Sugerimos também a qualificação linguística de que os dados genéticos ou biométricos devem estar expressamente ligados a um registo individual ou médico, a fim de incentivar a inovação e a investigação médica contínua. Grandes avanços médicos estão ocorrendo atualmente com o uso dos dados genéticos que são anonimizados frequentemente ou completamente randomizados, e agregados de modo a fazer com que os indivíduos fiquem virtualmente não identificáveis.

Dados Anonimizados

Entendemos que merece elogio a linguagem do projeto de lei que reconhece a anonimização como uma ferramenta importante para a proteção de dados. Acreditamos que a anonimização ajuda a diminuir o risco para os indivíduos e deve ser dispensada do projeto de lei. Os dados não identificados e anonimizados são aqueles que não podem ser razoavelmente identificados e certas medidas foram tomadas para proteger a pessoa contra o anonimato de forma razoável. Dados Descaracterizados e anonimizados são aqueles que não podem ser razoavelmente identificados e certas medidas foram tomadas para proteger a identificação da pessoa de forma razoável. Os dados pessoais deveriam incluir apenas dados ou conjuntos de dados processados relativos a indivíduos razoavelmente identificáveis. Isso elimina a incerteza e permite que as entidades responsáveis realizem avaliações de risco para cenários realistas, em particular beneficiando as pequenas empresas que têm menos recursos.

Muitos tipos de dados coletados são descaracterizados e/ou agregados de tal forma que seria necessário um grande gasto e tempo para determinar a identidade do indivíduo. Portanto, embora tecnicamente possível, é altamente improvável que o indivíduo seja identificado. Na verdade, em algumas circunstâncias, os dados adicionais teriam de ser recolhidos e mantidos para cumprirem os requisitos deste projeto. No entanto, limitando-se a linguagem será possível encorajar um maior uso do anonimato.

Dados Públicos

Embora os dados publicamente disponíveis estejam sujeitos a direitos de acesso e obrigações de segurança de dados, os usuários desses dados não devem estar sujeitos a todos os requisitos de permissão. Desde que os dados são obtidos de fontes públicas, a permissão não é viável, já que o usuário não interage com o titular dos dados.

Como exemplo, para a lei argentina de proteção de dados (Seção 5, 2 (c)), os dados considerados públicos que limitam-se ao fornecimento de RG, números de CPF e INSS, profissão, data de nascimento e domicilio não necessitam de consentimento para serem fornecidos.

Processamento de Dados Pessoais

A Câmara de Comércio congratula a linguagem do projeto de lei que reconhece o interesse legítimo como base jurídica para o tratamento dos dados. O interesse legítimo protege dados individuais, o que exige que uma avaliação baseada em risco seja feita em cada caso. No entanto, no projeto atual, o uso de interesse legítimo poderia ser mais amplo.

Com o consentimento, deverá existir equilíbrio entre capacitar o indivíduo a exercer escolhas sobre sua privacidade e não sobrecarregar as políticas de privacidade com muitos detalhes que poderão confundir os consumidores ou fazê-los ignorar completamente as políticas. Como aqui mencionado, os requisitos para o consentimento são restritivos, e dificultariam muitas empresas amplamente aceitos às práticas comerciais e utilização de dados comerciais, aumentariam os custos para as empresas e os consumidores, e privariam os consumidores de produtos desejados e serviços. Embora o consentimento seja um ponto importante para o processamento de dados, ele não deve ser o único motivo para o processamento dos dados.

A prestação de serviços aos consumidores por meio de canais digitais exige um quadro de consentimento flexível que permita a circulação de dados tendo em conta o risco potencial de prejuízo para o titular dos dados. Por exemplo, os dados autorizados por órgãos reguladores, certificados por padrões de segurança de dados e regidos por finalidades específicas ou limitações de uso implicam muito menos risco do que a transferência de dados pessoais para outras instituições sem fins legítimos ou específicos. Portanto, o consentimento implícito ou informado do consumidor para uso e transferência de dados, em vez de consentimento expresso ou afirmativo, é um padrão apropriado. Esse consentimento proporcional deverá ser criado para evitar aumento de custos, limites ao acesso à melhor tecnologia disponível e redução da prestação de serviços.

Além disso, as organizações precisam proteger seus dados, propriedade intelectual, sistemas e redes de TI e outros ativos contra usos fraudulentos ou ataques à segurança cibernética. Tais medidas exigem frequentemente o tratamento de dados pessoais, incluindo aqueles que podem estar envolvidos em atividades fraudulentas ou ataques à segurança cibernética. A obtenção do consentimento nessas circunstâncias prejudicaria a finalidade do processamento. Esses exemplos de processamento também poderiam ser baseados em uma exceção de interesse legítimo.

Entendemos que merece elogio a remoção da linguagem de consentimento expresso do projeto de lei. O consentimento expresso deve ser limitado a situações em que o consentimento é a única base para a coleta e processamento de dados. As disposições relativas ao consentimento em geral deverão considerar o contexto do processamento de dados e permitir uma abordagem flexível para evitar confundir os consumidores com pedidos repetidos de consentimento em situações triviais.

Para encorajar a inovação e evitar custos desnecessários para as empresas, sugerimos que, para dados menos sigilosos, exista um padrão de consentimento informado, implícito, de exclusão voluntária ou implícito. A abordagem do consentimento orientada pelo contexto e baseada em risco tem obtido sucesso em todo o mundo. Também pode ser benéfico permitir um tratamento legítimo baseado em interesses de dados sigilosos em contextos em que a obtenção do consentimento seria impossível ou impraticável.

O consentimento deve ser implícito para práticas de coleta e uso de dados comumente aceitas, como processar uma transação solicitada pelo consumidor, gerenciamento de riscos, segurança de dados e análise de desempenho de serviços e aplicativos. Sugerimos também, que

para transferências para fins de processamento e recuperação de desastres, seja no país ou fora dele, providências sejam tomadas para permitir transferências, sem o consentimento do consumidor, de acordo com cláusulas contratuais que permitam exigir ao processador que atenda a salvaguardas administrativas razoáveis.

Além disso, para a utilização de dados pessoais não é relevante ter um consentimento específico; ao invés disso, e como mencionado anteriormente, o consentimento deve ser dado de forma informada e inequívoca, equilibrando assim a proteção dos dados pessoais e a inovação. A ideia subjacente ao consentimento específico já está coberta pelos princípios que regem o tratamento de dados pessoais, como a boa fé (que compreende a finalidade e os princípios da adequação). De acordo com o projeto de lei atual, uma pessoa só pode processar dados pessoais para uma finalidade específica. Neste contexto, as empresas seriam forçadas a obter consentimento específico para cada serviço adicional oferecido, prejudicando grandemente a experiência do usuário e inibindo a inovação.

O relatório da Câmara de Comércio, *Designing a Data Risk Governance Approach for Tomorrow* (anexado com estes comentários), propõe um modelo adequado de linguagem de consentimento, examinando várias jurisdições para determinar as melhores práticas globais.

De acordo com o projeto de lei, o consentimento pode ser revogado. Isto significa que o titular dos dados poderá solicitar que uma empresa não processe os seus dados a qualquer momento. Se um titular dos dados se opuser ao processamento de dados pessoais, ele poderá exigir que o processador de serviços cancele determinados serviços on-line ou restrinja o acesso a determinado conteúdo. Assim, encorajamos a adição de uma exceção ao artigo 9, Item IV, em relação à oposição ao processamento, quando este for essencial para o cumprimento de uma obrigação legal ou contratual ou quando o processamento de dados for inerente à natureza da Transação ou serviço fornecido.

Autoridade Competente [Data Protection AuthorityAuthority, DPA (Autoridade de Proteção de Dados)]

Entendemos que é positiva a referência do texto à criação de uma autoridade competente para supervisionar a implementação do regulamento de proteção de dados no Brasil. O projeto de lei não esboça atualmente como uma autoridade de proteção de dados será criada, o que é compreensível devido aos critérios formais de iniciativa para propor tal matéria. Olhando para o futuro, quando da criação da autoridade, incentivamos o governo brasileiro a mostrar liderança em termos de melhores práticas internacionais. A fim de responder plenamente aos desafios da proteção de dados, qualquer organismo competente deve ser totalmente financiado, dotado de pessoal e independente.

A aplicação plena da lei após aprovação do projeto dependerá de uma autoridade de funcionamento independente, competente e bem financiada. Cumprir os novos requisitos exigirá recursos financeiros e monetários extensivos e as empresas precisarão de um período de tempo adequado para garantir uma implementação adequada. Caso haja maneira de suprimir o vício de iniciativa para se determinar no projeto de lei a criação da autoridade, sugerimos que o texto final especifique que a data de entrada em vigor não ocorrerá até um mínimo de 2 (dois) anos e

após a criação ou designação de uma autoridade competente em pleno funcionamento. Será necessário tempo para as mudanças técnicas e operacionais necessárias para a conformidade, e também sugerimos alocações mínimas de tempo para a implementação de quaisquer requisitos futuros desenvolvidos pela autoridade competente. Ressaltamos a importância de tempo apropriado para o cumprimento de quaisquer requisitos adicionais, conforme determinado pelo órgão competente.

A Câmara de Comércio publicou um relatório, Seeking Solutions: Atributos de Autoridades de Proteção de Dados , que esboça sete itens chave dessas autoridades e oferece exemplos de como elas os incorporaram. Os sete itens são:

1. Promova a Educação e Consciência
2. Buscar Feedback
3. Ofereça Orientação e assistência
4. Aja legalmente
5. Aja com transparência
6. Esforce-se pela Coordenação e Cooperação
7. Seja hábil em negócios e em tecnologia

Esse documento está sendo traduzido para o Português e maiores informações poderão ser requeridas ao Conselho Empresarial Brasil-Estados Unidos, que compõe a Câmara de Comércio. O contato pode ser feito por meio de João Barroso, senior advisor no Brasil, email jbarroso@brazilcouncil.org.

Transferências Internacionais

Entendemos que é positivo o projeto de lei a respeito das transferências internacionais, reconhecendo uma série de mecanismos legítimos, tais como cláusulas contratuais padrão e padrões corporativos globais. Reconhecer esses mecanismos permite o fluxo contínuo de dados e posiciona o Brasil como um participante ativo na economia digital global.

O Brasil deve observar o sistema de Regras de Privacidade Entre Fronteiras (Cross-Border Privacy Rules, CBPR) da APEC[3], que reconhece mecanismos mais legítimos, como marcas de privacidade e códigos organizacionais de conduta que são certificados por uma autoridade competente ou terceiro. O Brasil poderia permitir que organismos de certificação reconhecidos autorizassem tais mecanismos, como os Agentes de Responsabilidade no sistema CBPR da APEC, para evitar problemas de aprovação dentro desse órgão. O relatório da Câmara de Comércio Globally Connected, Locally Delivered: O Impacto econômico dos serviços de TIC entre fronteiras destaca especificamente a importância da adoção de um quadro de proteção de dados baseado em risco que permita transferências internacionais, o que atrairá investimento estrangeiro direto para o Brasil.

Outra opção poderia ser simplesmente estabelecendo que as transferências de dados internacionais possam ocorrer livremente, sujeito aos princípios estabelecidos nesta lei. A necessidade de aprovação prévia para a transferência internacional de dados é bastante onerosa e não é adequada no contexto de uma economia global onde as transferências internacionais de

[3] Veja http://www.cbprs.org/ Para obter mais informações sobre o regulamento de privacidade entre fronteiras da APEC.

dados são necessárias e fazem parte das operações comerciais diárias da empresa. As transferências internacionais de dados são responsáveis pela ascensão de novos negócios em todo o mundo e pela economia digital. A Internet e a sua capacidade de permitir o livre fluxo de informações são um grande impulso para o comércio econômico e novos modelos de negócios que operam exclusivamente on-line. Se houver necessidade de consentimento expresso ou autorização formal da autoridade competente para transferências internacionais de dados, operações diárias de negócios, bem como o desenvolvimento, o crescimento e a difusão da inovação e das novas tecnologias, como a Internet das Coisas (Internet of Things, IoT), poderia ser negativamente impactado.

Outras leis coletivas de proteção de dados nos países latino-americanos permitem transferências internacionais de dados para países que podem não fornecer o mesmo nível de proteção, mediante a obtenção de um consentimento informado e inequívoco da pessoa que autoriza a entidade responsável a fazer essa transferência internacional. Isso inclui as leis coletivas de proteção de dados do México, Peru e Colômbia, entre outros. Acreditamos que esta também possa ser uma solução prática e razoável.

Acreditamos que os conceitos de "adequação" a nível de país são frequentemente problemáticos, inconsistentes e atrapalham a inovação. Ao limitar as transferências de dados para os países em uma lista, o Brasil terá mais dificuldade em interagir com a economia digital global e privará seus cidadãos dos produtos e serviços que eles procuram. É essencial que todas as determinações sejam feitas de forma transparente e oportuna. Também sugerimos a criação de diretrizes que requeiram a coleta de contribuições dos interessados, a fim de criar uma avaliação totalmente informada.

Embora uma "autoridade competente" seja responsável pela avaliação do nível de proteção de dados de outros países, não está claro em que momento a autoridade competente será designada ou durante quanto tempo essa entidade precisará estar plenamente funcional. Além disso, levará tempo para avaliar os níveis de proteção de dados de outros países, criando incerteza contínua. Sugerimos o fornecimento de orientação de que os mecanismos de transferência de dados e as melhores práticas atualmente inseridas no projeto de lei permaneçam válidas até que tais determinações possam ser feitas. Também é essencial que todas as determinações sejam feitas de forma transparente e oportuna.

Responsabilidade

Uma empresa que viole uma lei deve ser responsabilizada. Acreditamos que a empresa que coletou e processou os dados deve ser responsável pelos danos causados por essas ações. Não deverá haver qualquer responsabilidade conjunta como atualmente prevista no projeto de lei. Da mesma forma, as entidades que pertencem ao mesmo grupo econômico não devem ser solidariamente responsáveis pela violação. Em última análise, a parte das empresas do mesmo grupo econômico pode ser responsabilizada pela violação de qualquer disposição como uma subsidiária. No entanto, é a empresa que violou a lei que deve ser responsabilizada.

Prazo para acessar, bloquear, cancelar e dissociar dados de titulares de dados

O prazo de 7 (sete) dias para que o titular dos dados solicite o acesso aos seus dados, tal como estabelecido no artigo 18 do projeto de lei, é muito pequeno para que as empresas os encontrem. A este respeito, sugerimos uma adaptação de curto para longo prazo, por exemplo, 60 (sessenta) dias.

Sanções

Encorajamos a remoção das disposições da seção do projeto de lei a respeito das sanções relacionadas à suspensão total ou parcial das atividades de tratamento de informações pessoais; ou à proibição total ou parcial das atividades de tratamento de informações pessoais.

Algumas sanções são desproporcionais. Por exemplo, as sanções que encerram as operações de uma base de dados ou suspendem/proíbem o processamento de dados, mesmo que por um período de tempo limitado, encerrariam as atividades comerciais, prejudicando os consumidores. Tal medida poderia limitar o investimento e os serviços oferecidos no Brasil devido à natureza onerosa deste regulamento. Qualquer tipo de sanção que queira suspender o processamento de dados deverá apenas afetar os dados recolhidos ao violar a lei e não todos os dados recolhidos e armazenados numa determinada base de dados.

Entrada em vigor

Devido à complexidade da implementação deste projeto de lei, e devido as leis de proteção de dados da União Europeia, recomendamos que este projeto de lei entre em vigor o mais tardar em dois (2) anos após a sua aprovação. Será necessário tempo para as mudanças técnicas e operacionais necessárias para o cumprimento. A lei final de proteção de dados também deve incluir uma "cláusula de anterioridade" que detalha seus impactos de coleta de dados de forma prospectiva e não retroativa. Ressaltamos a importância de tempo apropriado para o cumprimento de quaisquer requisitos adicionais, conforme determinado pelo órgão competente.