Comentários do Information Technology Industry Council em Resposta à solicitação feita pela Comissão Especial da Câmara de Deputados encarregada de discutir o projeto de lei sobre tratamento e proteção de dados

O *Information Technology Industry Council* (ITI), porta-voz global do setor de tecnologia, agradece a oportunidade concedida por esta Comissão Especial de apresentar os seguintes comentários sobre a discussão do Projeto de Lei para o tratamento e proteção de dados pessoais.

O ITI é o porta-voz, defensor e um dos principais líderes na indústria global de Tecnologia da Informação e Comunicação (TIC)[1]. Os membros do ITI recebem informações pessoais de seus usuários e assumem com seriedade sua obrigação de proteger a privacidade de seus clientes. Esses membros possuem operações globais e, portanto, estão sujeitos a arcabouços regulatórios de privacidade ao redor do mundo.

É com essa profunda experiência que o ITI vem encorajando os governos de diversos países a desenvolverem arcabouços regulatórios de privacidade para proteger as informações pessoais de maneira equilibrada, de forma a fomentar a inovação, permitindo o crescimento do comércio e facilitando o livre fluxo de informações. Esse arcabouço regulatório apoiaria o crescimento econômico do Brasil, permitindo uma maior competitividade das empresas brasileiras, inclusive daquelas de pequeno e médio porte (PMEs), aperfeiçoando a capacidade do Brasil no que diz respeito à indústria de TIC e atraindo investimentos deste setor. Isto também auxiliaria o Brasil a atingir sua meta de se tornar um participante global nos setores de software e serviços de TI e alcançar suas metas estabelecidas no *TI Maior*, no que diz respeito ao crescimento das exportações de software e de serviços de TI, chegando a US$ 20 bilhões até 2022.

Como de conhecimento de todos, o Projeto de Lei nº. 4.060/2012 foi o primeiro documento submetido à Câmara dos Deputados que contemplava uma proposta para o tratamento e proteção de dados pessoais no país. Posteriormente, outros projetos de lei sobre a matéria foram apresentados à Câmara dos Deputados. Nesse sentido, considerando-se a importância desse assunto (proteção de dados pessoais), foi constituída uma Comissão Especial, centralizando a discussão de todos esses textos. Grande parte dos debates da Comissão Especial teve por objeto o Projeto de Lei nº. 5.276/2016, em consequência do amplo processo de consulta de pública que o envolveu.

Portanto, a ITI preparou comentários específicos sobre o Projeto de Lei nº 5276/2016, focando no que acreditamos ser os pilares de um arcabouço regulatório de sucesso e de apoio para o desenvolvimento econômico, e conhecedores da realidade da moderna economia impulsionada pelos dados.

[1] Lista com os membros do ITI encontra-se anexa a esta carta.

1101 K Street, NW Suite 610
Washington, D.C. 20005
(202) 737 - 8888 | www.itic.org

O ITI agradece a oportunidade de focar em diversos conceitos relevantes do Projeto de Lei nº 5.276/2016, que poderiam ser objeto de um debate mais profundo bem como de esclarecimentos e revisões ao referido texto.

A. ESCOPO DA LEI (ARTIGO 3º)

O Projeto de Lei nº 5.276/2016, conforme atualmente proposto, traz um escopo um pouco ampliado com relação à aplicação da lei, incluindo quando (i) a operação de processamento do dado for realizada no território nacional, (ii) a atividade que requer o tratamento de dados tiver por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional, ou (iii) os dados pessoais objeto do tratamento tiverem sido coletados no território nacional.

Acreditamos que esse escopo amplo possa representar desafios significativos às empresas que buscam ofertar serviços no mercado online, onde, por vezes, é um desafio identificar onde o usuário está, de fato, consumindo os serviços. Conforme atualmente redigida, a lei em questão concederia jurisdição a atividades que ocorrem no Brasil, mas que envolvem cidadãos estrangeiros, e não residentes no Brasil. Dessa forma, recomendamos a exclusão do inciso (i) que poderia dissuadir as organizações de selecionar o Brasil como seu centro de operações. O Brasil ocupa posição privilegiada no que diz respeito à exportação de serviços de processamento, especialmente para a região, podendo assumir a liderança da exportação de serviços no setor tecnológico, causando séria preocupação de que esse potencial possa ser prejudicado com a adoção de uma legislação tão restritiva.

Cumpre notar que a área de exportação de serviços de tratamento de dados pode ser bastante relevante para o crescimento da economia brasileira, e é desejável ter uma estrutura legal atraente para acolher esses investimentos e ser considerada na formulação da política pública.

Sugerimos que esse escopo amplo seja revisado e limitado para que o escopo da lei seja exclusivamente quando (a) o responsável pelo tratamento dos dados tiver um estabelecimento permanente no Brasil e (b) os residentes no Brasil forem alvos específicos e os dados forem coletados pelo ou em nome desse estabelecimento. Nesse sentido, sugerimos que o Artigo 3º do Projeto de Lei nº 5.276/2016 seja alterado, para que os responsáveis pelo tratamento de dados no país somente estejam obrigados a coletar e processar dados pessoais de cidadãos brasileiros, como segue:

"Artigo 3º. Esta Lei aplica-se a qualquer responsável pelo tratamento de dados instituído de acordo com a lei brasileira, desde que:
I – a pessoa jurídica tenha estabelecimento permanente no Brasil e os dados pessoais objeto de tratamento forem coletados no território nacional;
II – a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional."

A. DEFINIÇÕES (ARTIGO 5º)

(i) Dados Pessoais (Artigo 5º, I)

A definição proposta para dados pessoais é expansiva e ambígua, enquadrando quase todas as informações como dado pessoal. Da forma como redigida, ela incluirá dados que não identificam um indivíduo especificamente, uma vez que as palavras "relacionado a" incluirão dados que não podem ser razoavelmente usados para identificar razoavelmente um indivíduo. A definição de dados pessoais não deve incluir informações que não tenham conexão razoável com um indivíduo específico e não deve incluir dados que tiveram sua identificação removida ou anonimizados no contexto específico de determinado uso.

Qualquer definição que seja excessivamente ampla ou crie incerteza deve ser evitada, não só sob a perspectiva da certeza jurídica, a qual já justificaria essa necessidade, mas também face aos inúmeros benefícios que os modelos comerciais impulsionados por dados têm para o processo de transformação digital das economias modernas.

Os critérios para a definição de dados pessoais devem estar vinculados ao potencial de tais dados para identificar de forma eficaz uma determinada pessoa e, assim, afetar a sua privacidade. Nos Estados Unidos, por exemplo, o conceito de "*personally identifiable information*" (PII) é amplamente utilizado e é baseado na probabilidade e facilidade com que uma determinada peça de informação poderia resultar na identificação de uma determinada pessoa. A Lei de Proteção de Dados Pessoais de Cingapura é outro exemplo dessa abordagem baseada em risco para a definição de dados pessoais. A lei considera dados pessoais qualquer informação sobre um indivíduo que "*pode ser identificado a partir desses dados*" ou outros dados que possam ser razoavelmente acessados, ao invés de conter um comando amplo sobre o potencial de identificação por meio dos dados.

A este respeito, o ITI sugere a seguinte redação para a definição de Dados Pessoais: ***"qualquer informação que razoavelmente identifique de forma precisa uma pessoa natural"***.

(ii) Dados Sensíveis (Artigo 5º, III)

Diversos países não contemplam uma definição específica para dados sensíveis, reconhecendo o fato de que vários tipos de dados pessoais podem ser considerados mais sensíveis ou menos sensíveis de acordo com o contexto no qual sejam utilizados, e, pelo contrário, adotam uma abordagem baseada em risco, criando obrigações mais rígidas para circunstâncias mais sensíveis de uso dos dados. Essa abordagem proporciona maior flexibilidade e está bem equipada para minimizar seu risco para as pessoas.

Contudo, se o Brasil optar pela adoção de uma categoria específica de dados sensíveis, recomendamos que os tipos de dados considerados sensíveis sejam restritos a uma lista fechada, como apresentado na lei, evitando termos demasiadamente vagos e qualquer confusão que poderia categorizar como "sensível" qualquer tipo de informação pessoal, e que as disposições de consentimento relacionadas aos dados sensíveis não se tornem tão restritivas que impeçam o uso desses dados – com salvaguardas apropriadas – para usos benéficos. Isto poderia rapidamente se tornar uma desvantagem competitiva em relação a regimes mais equilibrados e irá não só restringir a capacidade de operação das empresas estabelecidas, como também impedirá o ambiente certo para a inovação no país.

Em geral, os legisladores e reguladores brasileiros deveriam reconhecer que o tratamento de dados categorizados como sensíveis pode ter resultados incrivelmente benéficos não só para o indivíduo como para a sociedade (como, por exemplo, no setor de saúde). As informações sobre saúde já têm sido utilizadas para metas maiores de política pública, buscando monitorar a disseminação de doenças no Brasil, como no caso do Zika vírus e dengue, bem como para reduzir significativamente o número de óbitos resultantes de infecções em hospitais brasileiros[2]. Para garantir que esses potenciais benefícios sejam usufruídos, aos legisladores cabe evitar qualquer perspectiva muito abrangente, habilitando diversos mecanismos ou fundamentos jurídicos para o tratamento de dados sensíveis.

Exigir consentimento expresso para o processamento de dados sensíveis impediria um grande número de usos benéficos de dados, onde o responsável pelo tratamento não está em condições de obter o consentimento ou quando o consentimento é negado sem um bom motivo em casos onde não há danos, por exemplo. Assim, incentivamos permitir o interesse legítimo como base para o processamento de dados sensíveis. Uma vez que as razões de interesse legítimo para

[2] Veja mais informações sobre este caso aqui: http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/cssf/noticias/audiencia-debater-sobre-software-de-tecnologia-de-prevencao-e-combate-a-infeccao-generalizada.

processamento exigem avaliação de riscos, bem como mitigações adequadas, em muitos casos, isto pode ser uma proteção maior dos dados pessoais do que o consentimento expresso pode ser. Além dos interesses legítimos, a base jurídica prevista nos incisos II (obrigação legal do responsável pelo tratamento) e VII (proteção da vida e segurança física) do Artigo 7º deve ser a fundamentação jurídica para o processamento de dados pessoais sensíveis. Da mesma forma, o processamento deve ser permitido nos casos em que o titular dos dados tenha fornecido dados voluntariamente como expressão de sua liberdade de expressão, consciência ou crença – por exemplo, quando alguém voluntariamente deseja divulgar sua religião ou orientação de gênero.

(iii) Anonimização ou Dissociação (Artigo 5º, XII)

Embora o conceito de minimização de dados tenha sido um princípio fundamental de privacidade e segurança por muitos anos, desenvolvimentos tecnológicos recentes nas áreas de *big data analytics* e *machine learning* devem incentivar os legisladores a revisitar a análise de custo-benefício e encontrar formas de aplicar este princípio de novas maneiras.

Uma vez que a minimização de dados é entendida como a prática de limitar a coleta de informações pessoais àquela que é diretamente relevante e necessária para realizar uma finalidade específica, ela entra em conflito com a definição de *big data analytics*, que é o processo de examinar grandes conjuntos de dados para descobrir padrões ocultos, correlações desconhecidas, tendências de mercado, preferências de clientes e outras informações úteis. Embora esses dois conceitos possam parecer irreconciliáveis, os reguladores devem ter a certeza de que não têm de escolher entre proteger os dados pessoais dos cidadãos ou explorar as descobertas inestimáveis que podem ser obtidas com a mineração de conjuntos de dados maciços.

Os reguladores japoneses reconheceram essa necessidade e recentemente atualizaram a Lei de Proteção de Informações Pessoais (APPI) japonesa, para incluir o conceito de informação anônima. "Informações anonimizadas" refere-se a qualquer informação sobre indivíduos a partir da qual todas as informações pessoais (ou seja, as informações que identificam um indivíduo específico, incluindo qualquer informação sensível) foram removidas. Se uma empresa anonimizar suficientemente as suas informações pessoais, está autorizada a divulgá-las a terceiros sem exigir o consentimento das pessoas em questão. Para garantir que os indivíduos tenham o direito de dar o "*opt-out*", solicitando assim a exclusão de tal possibilidade em relação aos seus dados, a lei exige que, antes de divulgar as informações anonimizadas a terceiros, uma empresa declare publicamente a natureza das informações incluídas nas informações anonimizadas e os meios pelos quais está compartilhando as informações anonimizadas.

Vários outros países têm trabalhado em mecanismos eficazes para desbloquear os benefícios do

processamento de dados anônimos, preservando os direitos dos titulares dos dados pessoais. O ICO do Reino Unido, por exemplo, estabeleceu uma abordagem avançada de risco[3] para anonimização e re-identificação. Eles reconhecem que o ideal de "anonimização perfeita" é supérfluo e muitas vezes inalcançável, e optam por incentivar as empresas a empregarem medidas técnicas e contratuais para mitigar o risco até que a probabilidade de re-identificação seja remota.

O ITI sugere que os dados ainda devem ser considerados anônimos para os propósitos desta lei, mesmo que possam ser re-identificados por meios "razoáveis", se a anonimização for acompanhada de outras proteções processuais, administrativas e legais contra a reversão da anonimização ou re-identificação. Recomendamos que a lei reconheça explicitamente a utilização de compromissos processuais, administrativos e legais (tais como compromissos contratuais executáveis com terceiros e prestadores de serviços para não re-identificar dados anonimizados) para incentivar as empresas a adotar tais medidas. Esta é uma forma eficaz de promover melhores práticas de privacidade e segurança cibernética sem sobrecarregar as novas indústrias que dependem de grandes dados.

O ITI sugere a seguinte adaptação à definição de "anonimização":

> "*XII - anonimização: qualquer procedimento por meio do qual um dado não pode mais ser razoavelmente associado, direta ou indireta, a um indivíduo identificado ou identificável*."

Além disso, a ITI sugere que o processamento de dados anônimos seja expressamente excluído do âmbito de aplicação da lei:

> "*Art. 4. Esta Lei não se aplica ao processamento de dados:*
> *[...]*
> *IV - que é anonimizado.*"

B. PRINCÍPIOS

(i) Princípio da Necessidade (Artigo 6º, III)

Este princípio é inconsistente com a habilitação de usos benéficos inovadores de dados e a limitação do que é o "mínimo necessário" é subjetiva, e pode não ser o mais interessante para os consumidores. Além disso, o princípio pode não comportar as expectativas dos usuários de que as

[3] Anonymization: Managing Data Protection Risk Code of Practice (ICO, 2012).

empresas tratem seus dados de forma a aprimorar operações e em conexão com produtos e serviços aprimorados.

Ademais, por exemplo, no caso de autenticação de um titular de dados para acessar dados anteriormente coletados, os titulares dos dados seriam mais bem protegidos pela coleta de dados através de vários pontos de autenticação para garantir que o acesso não seja concedido de forma errônea.

Portanto, recomendamos veementemente a revisão da proposta para excluir esse princípio de maneira integral, a fim de garantir que o Brasil receba um ecossistema digital inovador e vibrante, que necessariamente seja baseado no uso de dados.

(ii) Princípio do Acesso (Artigo 19)

O princípio contido no Artigo 19 é problemático por uma série de razões. Primeiro, exigir o fornecimento de dados pessoais "imediatamente" poderá não ser, em muitos contextos, uma iniciativa viável e poderia também, apresentar um risco para a segurança e integridade da informação.

O Parágrafo 1º do Artigo 19 exige que os dados pessoais sejam armazenados em um formato que permita o exercício "imediato" do direito de acesso. Incitamos os legisladores brasileiros a considerar as implicações de tal exigência. Além disso, pedimos esclarecimentos sobre se este parágrafo refere-se ao acesso fornecido ao titular dos dados, ou às autoridades responsáveis pela aplicação da lei. Ademais, o requisito de que os dados sejam fornecidos imediatamente em um "formato simplificado" levanta preocupações sobre como as empresas podem cumprir esta disposição e suas implicações na segurança. Não está claro o que pode contar como um "formato simplificado", e se isso requer a decriptação de informações criptografas ou cria uma obrigação para as empresas criarem uma interface técnica para ajudar a acessar os dados sob demanda.

Conforme previsto no Projeto de Lei, é muito difícil compreender o alcance desta exigência, suas implicações para a privacidade e segurança, e como ela pode ser implementada pelas empresas.

C. CONSENTIMENTO LIVRE, INFORMADO E INEQUÍVOCO

O consentimento é um modelo importante de proteção de informações pessoais que busca capacitar os titulares dos dados para tomar decisões informadas sobre se e como seus dados são usados. Nos casos em que as transações envolvendo dados estão claramente definidas e existe uma

relação direta entre titulares dos dados e as organizações com as quais eles lidam, este modelo é amplamente bem-sucedido e confiável para equilibrar os direitos das pessoas interessadas com organizações que desejam usar os dados.

No entanto, com o surgimento de inovações que dependem dos últimos desenvolvimentos em *cloud computing*, *big data* e Internet das Coisas (IoT), o ambiente é radicalmente diferente. Intercâmbios tradicionais e isolados de dados estão sendo substituídos por fluxos de dados por meio de sistemas distribuídos, dificultando a compreensão de quais organizações estão processando seus dados e para quais fins.

Isso levou os reguladores de privacidade a repensar a ênfase colocada no consentimento como um fundamento legal para a proteção de dados e um desejo crescente de buscar soluções que evitem o ônus excessivo que os regimes focados em consentimento podem impor tanto em organizações como em indivíduos[4]. Uma solução importante é a inclusão de razões de interesse legítimo para o processamento de dados, o que coloca o ônus da responsabilização e transparência nas organizações que usam os dados.

Por isso, elogiamos tanto a redação proposta para o consentimento inequívoca e informadae a inclusão do "interesse legítimo" como fundamentação jurídica para o processamento de dados pessoais no Projeto de Lei nº 5276/2016. Por um lado, garante que os direitos dos usuários sejam protegidos. Por outro lado, permite flexibilidade suficiente para garantir que a natureza dinâmica da Internet não seja, de forma alguma, limitada.

Também recomendamos que quaisquer ajustes aos requisitos de consentimento feitos pela autoridade competente como parte de suas funções estabelecidas no Art. 9º, § 7º, reflitam de forma semelhante essa flexibilidade e evitem impor obrigações gerais para tipos específicos ou métodos de coleta de consentimento.

D. AUTORIDADE COMPETENTE

O Projeto de Lei nº 5.276/2016 delega muitos requisitos para a ainda não criada "autoridade competente". Esta delegação de requisitos pode alterar fundamentalmente as exigências do Projeto de Lei proposto criando, inclusive, prazos imprevistos e gerando consequências inesperadas e maléficas para consumidores e empresas.

Negócios precisam de previsibilidade para desenvolver sistemas que sejam flexíveis para atender às

[4] Policy and Research Group of the Office of the Privacy Commissioner of Canada, May 2016.

adaptações tecnológicas e os consumidores precisam de garantias de que os seus dados serão protegidos adequadamente diante de uma tecnologia que se transforma rapidamente. Portanto, sugerimos que quaisquer requisitos futuros sejam elaborados em conjunto com a participação significativa das partes interessadas (*stakeholders*).

Estamos especialmente preocupados com os requisitos do Parágrafo 5º do Artigo 8º; Parágrafo 4º do Artigo 19; Parágrafo 1º do Artigo 45; Artigos 47 e 48; e o Parágrafo Único do Artigo 56, onde é concedido à autoridade competente o poder para determinar novas obrigações de conformidade que possam exigir adaptações técnicas relevantes nas operações de uma empresa, que exigirão tempo para sua implantação e poderão demandar investimentos substanciais, criando uma barreira à entrada de novos e pequenos agentes nesses mercados. As empresas podem enfrentar grande incerteza enquanto aguardam requisitos adicionais, e esse tempo de espera pode limitar a aplicação das tecnologias mais recentes, prejudicando tanto o consumidor brasileiro como a economia do País.

O ITI insta veementemente que qualquer aplicação da lei seja limitada a uma única agência ou Departamento do Governo Federal. A aplicação da lei por uma agência assegurará interpretações consistentes e certeza regulatória, que são elementos críticos para que um arcabouço regulatório funcione bem. Embora reconheçamos os desafios orçamentários decorrentes do estabelecimento de uma nova agência de fiscalização, defendemos uma nova Agência independente de fiscalização a nível federal. Uma agência de fiscalização independente, com exclusão de competência de qualquer outra autoridade para impor direitos de proteção de dados, seria o melhor veículo para garantir conhecimentos suficientes e a independência necessária para efetivamente aplicar a lei.

Observamos ainda que a criação de uma nova agência independente com seu próprio orçamento operacional não deve incluir as multas cobradas por violações às leis como parte desse orçamento operacional – tal arranjo criaria um incentivo de execução distorcido. Em vez disso, e de acordo com as práticas das mais eficientes Autoridades de Proteção de Dados que atualmente operam no mundo, a Agência Independente de Fiscalização brasileira deve ter um forte compromisso com a promoção da educação e conscientização, orientação e auxílio à comunidade regulada de forma consistente, utilizando-se sempre de discrição e bom senso. Deve também possuir um desejo contínuo de aperfeiçoamento, utilizando o *feedback* dado por seus regulados; criar processos colaborativos contando, mais uma vez, com o apoio dos já citados regulados; comprometer-se a ter uma atuação pautada pela transparência nos relacionamentos; e ganhando conhecimento em relação aos negócios em transformação e ao ambiente de tecnologia[5].

[5] Para um estudo aprofundado sobre as competências dos DPAs, favor verificar este relatório recente da U.S. Chamber:https://www.uschamber.com/report/seeking-solutions-attributes-effective-data-protection-authorities.

Gostaríamos de destacar que os Artigos 47 e 48 contêm dispositivos problemáticos que podem realmente prejudicar a segurança. Aparentemente, o Artigo 47 requer a "imediata" comunicação a autoridade competente de um incidente de segurança. Primeiramente, a necessidade de comunicação de uma violação ou de um incidente de segurança imediatamente, antes que o problema de segurança tenha sido, de fato, solucionado, parece-nos uma prática de segurança falha, pois poderá gerar a oportunidade para mais danos decorrentes de tal falha, criando oportunidade para eventuais hackers e criminosos. Em segundo lugar, tal aviso só deve ser exigido após a organização ter tido a oportunidade de determinar qual, se houver, impacto o incidente pode ter sobre a segurança e a privacidade dos titulares dos dados, para evitar uma notificação excessiva e desnecessária à autoridade, o que seria um mau uso dos recursos da agência.

O artigo 48 também parece exigir que a autoridade competente tenha a capacidade de duplicar e substituir as próprias investigações de uma empresa e o plano de resposta a incidentes após o incidente de segurança. Além de ser um exercício proibitivamente intensivo em recursos, isso provavelmente prejudicará os esforços da empresa para responder adequadamente a tais incidentes e criará uma dinâmica contraditória entre a autoridade competente e a empresa que foi vítima de um incidente de segurança como violação dados.

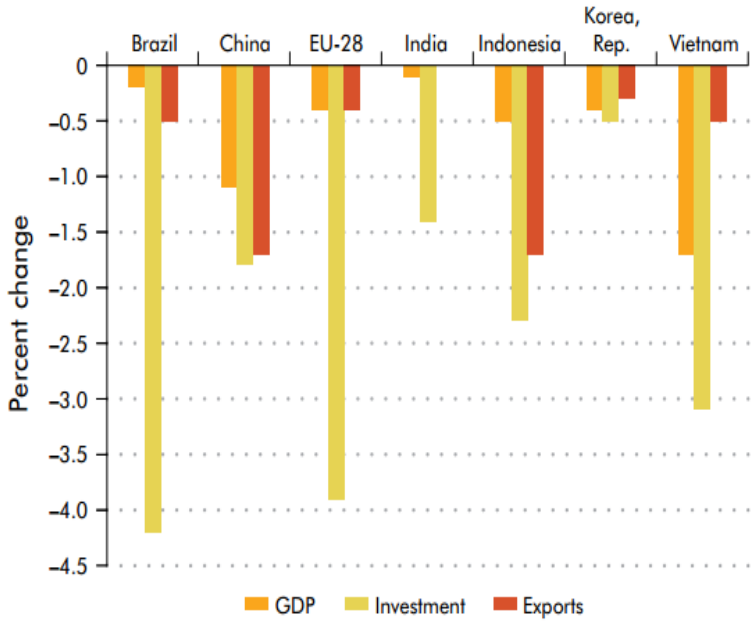
Em vez disso, a autoridade competente deve, como padrão, responsabilizar a empresa para determinar quando um incidente é suficientemente grave para exigir comunicação aos titulares dos dados e para realizar uma investigação interna sobre a violação ou procurar remediar sua causa. Além disso, não está claro como a autoridade competente estará em uma posição melhor do que a empresa para julgar a gravidade de um incidente de segurança, conforme contemplado neste artigo.

F. TRANSFERÊNCIAS INTERNACIONAIS DE DADOS (ARTIGOS 33-35)

O crescimento da internet serviu de combustível para o livre fluxo de dados e o livre fluxo de dados através das fronteiras viabilizou o maior avanço na facilitação do comércio desde a invenção da viagem aérea. Fica claro que os fluxos de dados transnacionais e a Internet como mercado ou canal de distribuição permitiram mais negociações transnacionais, maior competitividade e inovação.

O gráfico abaixo mostra o impacto negativo das restrições regulatórias sobre os fluxos de dados sobre o PIB e o investimento.

Mudanças no PIB, investimentos e exportações em virtude de restrições regulatórias aos fluxos de dados



Source: Bauer and others 2014. Data at http://bit.do/WDR2016-Fig6_5.

Note: The figure shows percentage changes according to simulations using a GTAP model. EU-28 = current member countries in the European Union; GTAP = Global Trade Analysis Project.

Ao adotar o modelo de "adequação" da União Europeia, que exige que a autoridade competente faça uma avaliação independente das leis de proteção de dados de outros países como principal base para a transferência internacional de dados, o Projeto de Lei nº 5276/2016 (Capítulo V – Artigos 33-35) cria obstáculos para os fluxos internacionais de dados, que são essenciais no mercado global e podem impedir o crescimento econômico no Brasil.

Além disso, o Projeto de Lei brasileiro propõe uma análise comparativa ainda mais rigorosa, que exclua as transferências de dados para outros países, a menos que os níveis de proteção de dados sejam "ao menos equivalentes" ao oferecido na legislação brasileira (Artigo 33). É bem verdade que o termo "adequada" é comumente interpretado como "equivalente" no modelo da União Europeia de legislação de privacidade, sem considerar se as regras de privacidade são de fato aplicadas. Enquanto isso, muitos outros países (incluindo parceiros comerciais importantes como os Estados

Unidos, Japão, Cingapura e Coreia) podem ter legislações de privacidade que protegem adequadamente os dados pessoais, mas que ainda não são consideradas como destinos seguros para dados pessoais da União Europeia[6] pois não foram considerados adequados no processo burocrático e/ou político.

Questionamos respeitosamente se o Brasil tomou em consideração os recursos significativos necessários para implementar o regime de "adequação" do modelo da União Europeia para as transferências internacionais conforme contemplado na Lei. Não só será caro, mas altamente ineficiente para a autoridade competente do Brasil analisar efetivamente as leis de proteção de dados de cada um dos parceiros comerciais do Brasil, bem como as práticas e cláusulas contratuais utilizadas por cada uma das empresas que atuam no ou com o Brasil, entidades empresariais ou cidadãos brasileiros.

Considerando tudo que foi mencionado acima, o foco em garantir que os dados não sejam transferidos para países que não possuem níveis de proteção "equivalentes", não garante, de fato, a proteção dos dados. **Uma estrutura legal deveria, preferencialmente, focar em como o responsável pelo tratamento dos dados vai assegurar que a organização que efetivamente receberá a informação – independentemente da jurisdição – tratará a informação de forma similar, apresentando a melhor garantia de um tratamento apropriado.**

Nessa estrutura, o responsável pelo tratamento dos dados é encarregado de implementar mecanismos que exijam que terceiros, a quem os dados são transferidos, tratem os dados pessoais de acordo com os compromissos de privacidade exigidos. Esse modelo de "responsabilidade" exige que a parte cedente tome as medidas adequadas para assegurar que a parte cessionária seja capaz de atender os compromissos de privacidade exigidos, via obrigação contratual, melhores práticas ou outros compromissos.

Diversos mecanismos podem ser usados para assegurar que essas garantias sejam aplicáveis às transferências. Embora o Artigo 34 sugira que alguns mecanismos serão permitidos para facilitar a transferência, como, ilustrativamente, cláusulas contratuais padrão ou as regras corporativas globais, o Projeto de Lei nº 5.276/2016 contempla a necessidade de aprovação das transferências feitas por meio desses mecanismos pelo órgão competente. Gostaríamos de alertar que a necessidade de aprovação prévia para transferências é administrativamente onerosa, e, portanto,

[6] *The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce*. Uma avaliação do impacto comercial do Regulamento Geral de Proteção de Dados (*General Data Privacy Regulation (GDPR)*) pelo Centro Europeu para Política Econômica Internacional (*European Centre for International Political Economy (ECIPE)*) para a Câmara de Comércio dos Estados Unidos. Consultar: https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf.

deverá ser fixada uma lista pré-aprovada das cláusulas contratuais padrão ou das regras corporativas globais, que não requerem aprovação adicional para cada uso.

Há uma gama de instrumentos que podem complementar ou que podem ser utilizados isoladamente como base para um modelo mais robusto e menos oneroso para as transferências de dados. São eles certificações, selos independentes e estruturas multilaterais, como, por exemplo, o sistema de regras de privacidade transfronteiriças do APEC (CBPRS) e outros mecanismos ou exceções disponíveis.

Um modelo possivelmente mais eficiente e produtivo que pode ser considerado pelo Brasil nessa discussão é o da Cooperação Econômica da Ásia e do Pacífico (*Asia Pacific Economic Cooperation* – APEC), na qual foi aprovada um Sistema de Privacidade[7] buscando promover o livre fluxo de informações entre as suas economias, baseado em órgãos de certificação e em programas terceirizados de credenciamento, que tem como lastro sua aplicação nacional. O Sistema de Privacidade da APEC é um sistema de privacidade que tem por base a responsabilização, fundamentado em uma abordagem baseada em princípios e, portanto, pode ser implementado em diversos países por meio de ou em conjunto com suas próprias legislações que dispõem sobre privacidade. A estrutura multilateral tem por objetivo aperfeiçoar o compartilhamento de informações entre as agências regulatórias e o governo e facilitar a transferência segura de informações entre as economias, mantendo, ao mesmo tempo, estabelecendo um conjunto comum de princípios de privacidade e proporcionando assistência técnica a essas econômicas que ainda não tenham abordado a privacidade sob a perspectiva regulatória ou política.

Os princípios fundamentais da estrutura dos CBPRs da APEC são flexíveis o suficiente para serem adotados em uma escala mais ampla. O seu sistema de 'responsabilização' torna aquele que coletou originalmente os dados como legalmente "responsável" por esses dados, independentemente de virem a ser transferidos, bem como os cessionários proporcionalmente ao uso ao qual eles dão aos dados. A lei imputa ao responsável pelo tratamento dos dados a responsabilidade por garantir que aquele que receberem estes dados, aqueles para quem os dados são transferidos no exterior, observem os mesmos princípios estabelecidos na política de privacidade do remetente.

A influência do sistema CBPR tem crescido e, na prática foi comprovado que esse Sistema é menos oneroso do que os demais (como, por exemplo, as Regras Corporativas Vinculantes da União Europeia, as quais, apesar de terem por base uma responsabilização corporativa, são bem onerosas,

[7] Sistema de Privacidade da APEC, ver http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx.

estão vinculadas a regras administrativas e sujeitas a um complexo processo de aprovação). Outro benefício desse Sistema é que os Agentes de Certificação recebem reconhecimento mútuo automaticamente dos demais países signatários, de forma que os titulares dos dados podem ser reparados de maneira pontual e eficaz sem a intervenção das autoridades nacionais tradicionais.

Alternativamente, a lei poderá permitir a livre transferência de dados internacionais, observado os princípios nela estabelecidos, permitindo às organizações escolher entre uma gama de ferramentas para a implementação de tal exigência, como, exemplificativamente, padrões da indústria, certificação ou cláusulas contratuais.

G. PENALIDADES ADMINISTRATIVAS (ARTIGO 15, PARÁGRAFO ÚNICO E ARTIGO 52)

As penalidades previstas entre os incisos IV e VII do Artigo 52 (bloqueio de dados pessoais, suspensão de operação e processamento de dados pessoais, cancelamento de dados pessoais e suspensão de operação de banco de dados) podem equivaler ao bloqueio no país das atividades de empresas baseadas majoritariamente no tratamento de dados.

Entre aqueles afetados por tais medidas desproporcionais estão não apenas plataformas que permitem a aproximação de empresas e clientes ou comunicação entre pessoas, mas também bancos de dados públicos e privados, plataformas de compartilhamento de informações urbanas e transporte de dados, plataformas de transporte ou hospedagem compartilhada, empresas financeiras ou de crédito, negócios baseados na Internet das Coisas (IoT)[8] – sendo que, na maioria das vezes, os maiores perdedores são os próprios cidadãos.

É importante ressaltar que qualquer sanção deve estar diretamente relacionada à natureza da violação e deve ser proporcional, levando em conta o dano resultante da infração. Por conseguinte, quaisquer sanções que possam afetar a capacidade de uma empresa de lidar com dados devem apenas relacionar-se potencialmente com os dados implicados que deram origem à violação.

Por conseguinte, as proibições internacionais relativas ao tratamento de dados não constituem sanções adequadas. Não seria viável, por exemplo, que uma organização continuasse a operar se fosse proibida a utilização de sua base de dados. Da mesma forma, impor uma suspensão de operar dados também efetivamente impediria uma organização de fornecer produtos e serviços às pessoas, o que pode ser extremamente perturbador. Além disso, esses tipos de sanções poderiam

[8] Nesse sentido, citamos empresas baseadas em agricultura de precisão, companhias de tecnológica médica, em suma, diversos ramos da indústria.

desencorajar as organizações de prestarem serviços no Brasil devido à natureza onerosa deste regulamento. 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 potencialmente os consumidores, assim como o Brasil.

A fim de evitar os excessos que podem ser gerados, devido a acordos para o bloqueio de atividades econômicas legítimas no país, nós sugerimos que sejam excluídos os incisos IV, V, VI e VII do Artigo 52; além disso, o inciso IV e o Parágrafo Único do Artigo 15 do Projeto de Lei nº 5276/2016.

Finalmente, os Artigos 34, 35 e 44 criam "responsabilidade solidária" entre o responsável e o operador dos dados pessoais. A responsabilidade solidária suscita uma série de preocupações com a responsabilização e a implementação da indústria. Para se certificar de que um alto padrão de proteção de privacidade seja mantido na economia baseada em dados, independentemente da localização, as empresas devem ser responsabilizadas pelo processamento dos dados que eles controlam ou que são realizadas em seu nome. Portanto, recomendamos que apenas os responsáveis pelo tratamento dos dados sejam responsabilizados por garantir o processamento de seus dados e dos seus operadores de acordo com os requisitos estabelecidos nesta lei.

H. SEGURANÇA DOS DADOS (ARTIGO 45, PARÁGRAFO 1º) E COMUNICAÇÃO SOBRE INCIDENTE DE SEGURANÇA (ARTIGO 47)

Uma legislação eficaz dispondo sobre a violação de dados não deve impor prazos estritos para a sua notificação e, em vez disso, deveria criar uma obrigação de notificação sem atrasos injustificados, uma vez que a empresa recolheu informações depois de ter conhecimento de um incidente. A lei deve igualmente aplicar normas distintas para a notificação das agências regulatórias e para a notificação dos titulares dos dados. Nos casos em que os dados comprometidos são criptografados ou tornados inacessíveis, tais violações de dados devem ser isentas dos requisitos de notificação.

É necessária uma quantidade tremenda de perícias, tomada de decisões e trabalho jurídico antes de determinar a natureza e o escopo de uma violação, para avaliar o risco de danos e determinar a forma apropriada de sua notificação. Reconhecendo a sofisticação dos hackers de hoje e a natureza desafiadora de uma investigação pericial de violação de dados, a legislação deve prescrever requisitos de tempo realistas, flexíveis e viáveis.

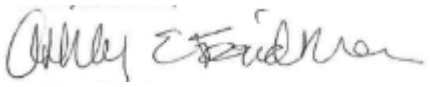
I. ENTRADA EM VIGOR (ARTIGO 56)

Considerando a complexidade dos procedimentos para sua implementação deste Projeto de Lei e

considerando o caso do Regulamento Geral de Proteção de Dados da União Europeia (GDPR), recomendamos que esta Lei entre em vigor, pelo menos, 2 (dois) anos após sua aprovação.

Mais uma vez agradecemos a oportunidade de enriquecer o debate acerca da proteção de dados pessoais no Brasil e ficamos a inteira disposição dos ilustres membros do Congresso Nacional para fornecer quaisquer esclarecimentos adicionais acerca das sugestões propostas.

Cordialmente,



Ashley Friedman
Director, Global Policy
Information Technology Industry Council

ITI

1101 K Street, NW Suite 610
Washington, D.C. 20005
(202) 737 - 8888 | www.itic.org