COMENTÁRIOS E SUGESTÕES PROPOSTAS PELA SEÇÃO AMERICANA DO CONSELHO EMPRESARIAL BRASIL-ESTADOS UNIDOS SOBRE O ANTEPROJETO DE LEI DO BRASIL PARA A PROTEÇÃO DE DADOS PESSOAIS
JULHO DE 2015

O Conselho Empresarial Brasil – Estados Unidos ("Conselho") é uma organização dedicada à promoção das relações econômicas e comerciais entre os dois países. A Seção Americana do Conselho representa as principais empresas norte-americanas com investimentos no Brasil e opera sob a égide administrativa da Câmara de Comércio dos EUA, em Washington, DC (vide www.brazilcouncil.org). A Seção Brasileira do Conselho é gerida pela Confederação Nacional da Indústria, em Brasília. Por meio desta, a Seção Americana do Conselho agradece a oportunidade de submeter comentários sobre o Anteprojeto de Lei do Brasil para a Proteção de Dados Pessoais.

Aplaudimos a iniciativa do governo brasileiro e os esforços do Ministério da Justiça no sentido de solicitar a opinião pública através do portal na web sobre tal importante regulamento, de uma maneira transparente e inovadora.

Apoiamos o desenvolvimento de regimes claros, consistentes de privacidade de dados que protejam os consumidores ao mesmo tempo em que promovem a inovação através do fluxo de dados ininterrupto. Este documento expõe sugestões detalhadas ao Anteprojeto de Lei para Proteção de Dados Pessoais ("Anteprojeto de Lei") para cumprir com estas metas. Estamos à disposição do Ministério da Justiça e do governo brasileiro de modo mais amplo para auxiliar no desenvolvimento de um Anteprojeto de Lei final que garanta a proteção da privacidade do público através da melhoria do regime de privacidade de dados no Brasil de uma maneira que seja eficiente, flexível, prática e que permita o desenvolvimento inovador contínuo, mantendo e aumente os benefícios para o consumidor, reguladores e negócios da mesma forma.

Na economia de informação dos dias de hoje, empresas de todos os portes e setores comunicam-se eletronicamente com seus funcionários, clientes existentes, clientes em potencial e parceiros comerciais em todo o mundo. Elas utilizam dados para estimular as vendas e o aumento de empregos, melhorar a produtividade, economizar, melhorar a eficiência e proteger os consumidores. Empresas sediadas no exterior investem milhões de dólares na economia brasileira e criam milhares de empregos. Os Estados Unidos e o Brasil estão na vanguarda da economia digital e o Conselho acredita que garantir o fluxo contínuo, seguro, ininterrupto de dados será um componente essencial

para inovação sustentável, crescimento e empregos. Como resultado, o Anteprojeto de Lei proposto deve ser desenvolvido de uma maneira que ofereça incentivos para investimentos nas práticas de proteção de privacidade e evite impedimentos desnecessários ao progresso.

Em muitos aspectos, o Anteprojeto de Lei ajuda a alcançar essas finalidades. Em outros, o Anteprojeto de Lei parece não conseguir atingir o equilíbrio correto, uma vez que muitas das proteções propostas são tecnicamente pouco práticas e terão consequências involuntárias que na verdade serviriam para retirar ou restringir os benefícios atualmente em vigor. Em muitos pontos, o Anteprojeto de Lei proposto é excessivamente prescritivo, o que restringe significativamente a inovação, aumenta os riscos para os consumidores e gera confusão, incerteza e dificulta sem proteções adicionais.

Existem vários conceitos amplos que impedem muitos dos problemas em potencial da proposta e, portanto, poderiam ser incorporados de forma liberal às mudanças no texto atual. Primeiramente, o Brasil deve pensar em refinar a proposta para permitir soluções com base em riscos que considerem a natureza e a finalidade dos dados sendo coletados. Em segundo lugar, o Anteprojeto de Lei deve ser estruturado de modo a incentivar o uso das melhores práticas internacionais visando a melhorar a interoperabilidade. Considerando o desejo do Brasil de assumir um papel de liderança mundial, incentivamos consultas a *experts* em privacidade e a consideração às melhores práticas existentes como aquelas encontradas na Organização para Cooperação e Desenvolvimento Econômico (OECD em Inglês[1]) e na Cooperação Econômica Ásia-Pacifico (APEC em Inglês[2])

Finalmente, o Anteprojeto de Lei proposto deve servir como oportunidade para incentivar empresas que já estão investindo e continuam a investir em segurança de dados. Ele deve reconhecer positivamente as empresas que já estão implementando políticas, procedimentos e normas condizentes com as melhores práticas da indústria para segurança de dados pessoas, permitindo o processamento de dados pessoais de modo contínuo entre fronteiras de países.

Nossa meta, com este documento, é oferecer sugestões práticas e específicas para ajudar a atingir as finalidades do Anteprojeto de Lei proposto. Começamos com alguns comentários gerais relativos às preocupações enfatizadas em termos gerais neste trabalho e a seguir oferecemos aditivos específicos com comentários fornecendo uma justificativa para o texto alterado.

Estamos à disposição para nos envolver, desenvolver e explicar melhor nossas sugestões e para trabalharmos juntos para alcançar uma solução que melhore a proteção à privacidade e que também estimule a inovação no Brasil.

---

1 Consulte http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm para as "Diretrizes da OCDE sobre a Proteção de Privacidade e Fluxos Transnacionais de Dados Pessoais."

2 Consulte http://www.cbprs.org/ para mais informações sobre o sistema de regras de privacidade transnacionais da APEC.

COMENTÁRIOS GERAIS

Gostaríamos de começar enfatizando várias preocupações e sugestões de aplicação geral.

Autoridade Competente

O Anteprojeto de Lei proposto deixa muitas exigências delegadas a uma "autoridade competente" ainda não criada. Estas provisões podem, essencialmente, alterar as exigências do Anteprojeto de Lei proposto, por períodos de tempo indeterminados causando danos e consequências inesperadas aos consumidores e empresas. Também não está claro como a autoridade competente se relacionaria com os reguladores que já estão incumbidos de fazer cumprir outras regulamentações sobre privacidade, uma vez que existem vários setores com fortes proteções à privacidade já em vigor.

Empresas precisam de previsibilidade para desenvolver sistemas que sejam flexíveis para atender as mudanças na tecnologia e os consumidores precisam de garantias que os dados pertencentes a eles sejam adequadamente protegidos em vista desta tecnologia em rápida mutação. Portanto, sugerimos que quaisquer futuras exigências sejam desenvolvidas com a participação significativa de partes interessadas e ofereçam uma período de tempo de implementação adequado.

Além disso, o Anteprojeto de Lei deve evitar mandatos de tecnologia excessivamente prescritivos, uma vez que eles podem resultar em inúmeros problemas, sendo um dos mais importantes a restrição a inovação e o aumento no risco para os titulares dos dados. As soluções também devem refletir a necessidade de transferências internacionais, bem como considerar tecnologias de rápido desenvolvimento, tais como a computação em nuvem. Destacamos nossa preocupação com as exigências descritas nos Artigos 13, 14, 28, 30, 40, 46, 47, dentre outros Artigos, onde é dado à autoridade competente o poder para instituir novas obrigações que podem necessitar de mudanças técnicas significativas para as operações de uma empresa e que demandarão tempo para implementação. As empresas podem enfrentar grandes incertezas enquanto aguardam as exigências adicionais, e este tempo de espera poderia limitar a aplicação de tecnologia mais nova e avançada.

Ao desenvolver a autoridade competente, incentivamos também o governo brasileiro a mostrar liderança nesta área através da aplicação das melhores práticas internacionais relativas à criação de uma autoridade para proteção de dados. Para atingir plenamente os desafios da proteção de dados, qualquer órgão competente deve estar totalmente financiado, equipado com funcionários qualificados e ser independente.

Finalmente, é importante que a data de implementação das provisões desta regulamentação esteja atrelada a criação de uma autoridade competente, funcional, independente e apropriadamente

financiada. Para estar em conformidade com as novas exigências da regulamentação serão necessários recursos técnicos e monetários abrangentes e as empresas precisarão de um período de tempo adequado para garantir a implementação da regra. Portanto, sugerimos que o projeto de lei final especifique que nenhuma data efetiva de implementação ocorra até o período mínimo de um ano após a criação ou indicação de uma autoridade competente plenamente funcional. Será preciso tempo para as mudanças técnicas e operacionais necessárias ocorrerem em conformidade e também sugerimos alocações de tempo mínimo para a implementação de quaisquer exigências futuras desenvolvidas pela autoridade competente.

Exigências de Responsabilidade Solidária

Ao longo do documento, propomos mudanças para refletir a necessidade de manter a flexibilidade nas obrigações contratuais entre o cedente e o cessionário, uma vez que ambas as partes nem sempre estão na posição de cumprir automaticamente com todas estas exigências; fazê-lo pode expor ambas as entidades a divulgar informações internas e de concorrência. Além disso, ambas as partes em contratos envolvendo o processamento de dados normalmente não fornecem materiais completos de auditoria um para a outra por uma série de motivos relacionados aos negócios, incluindo, em algumas circunstâncias, quando as partes podem ser concorrentes uma da outra em outros assuntos. Embora seja importante para as entidades responsáveis obter as informações necessárias para estarem em conformidade, as informações fornecidas podem ser limitadas e com frequência a melhor solução é deixar que as partes se expressem através de acordos contratuais entre elas. Um projeto de lei final deveria incentivar declarações de responsabilidade claras, mas, em última análise, deixar as partes livres para determinar a natureza da relação entre o cedente e o cessionário sobre como melhor cumprir com as exigências para proteção de dados através de um contrato. Em particular, destacamos preocupação com o texto atual dos Artigos 22, 30, 31, e com o Capítulo VII e com as mudanças sugeridas aqui que permitem o estabelecimento de uma relação contratual que garanta níveis adequados de proteção e promova, simultaneamente, a necessidade de soluções comerciais práticas.

Certeza Jurídica

Sugerimos esclarecer se o Anteprojeto de Lei tem a finalidade de se sobrepor às leis estaduais e outras leis federais no Brasil, incluindo aquelas leis relativas a dados financeiros e de saúde. Sugerimos que isto seja esclarecido, uma vez que uma estrutura jurídica transparente e consistente é fundamental para evitar confusão em relação a questões de implementação, conformidade e cumprimento. Isso criaria um melhor entendimento para as empresas, consumidores e governo.

Gostaríamos que houvesse um esclarecimento sobre a relação entre esta oportunidade de comentário e a seção de privacidade que é parte do Marco Civil da Internet no website do Ministério da Justiça. É nosso entendimento que este Anteprojeto de Lei proposto aplica-se a proteção da privacidade em todos os meios, enquanto o Marco Civil da Internet trata especificamente da atividade na Internet. Deve haver uma indicação clara sobre como as proteções à privacidade

antevistas por este Anteprojeto de Lei se relacionarão com as exigências introduzidas pela passagem do Marco Civil da Internet.

Distinção entre Responsável pelos Dados / Operador de Dados

A lei deve descrever uma distinção clara entre as obrigações que ela atribui a responsáveis pelos dados e aos operadores de dados. Os responsáveis pelos dados devem ter a obrigação principal de garantir a conformidade com a lei sobre a privacidade, enquanto os operadores de dados devem cumprir com as instruções do responsável pelos dados e garantir a segurança dos dados que processam. Estas são responsabilidades costumeiras atribuídas a responsáveis pelos dados e operadores de dados em leis de outros países sobre privacidade de dados.

Conforme descrito, as obrigações da lei parecem se aplicar igualmente tanto aos responsáveis pelos dados quanto aos operadores de dados na maioria dos casos. Isto criará incerteza e, com frequência, será impossível para os operadores de dados cumprirem tal lei, uma vez que a eles é permitido apenas atuar em nome dos responsáveis pelos dados e podem apenas tratar as exigências de privacidade de acordo com as instruções do responsável pelos dados. Em muitos casos, os operadores de dados não têm a permissão ou não se espera que eles conheçam os detalhes dos dados que estão tratando. Portanto, recomendaríamos que várias disposições na lei, incluindo o que dispõe os Capítulos II, III, IV e V, sejam aplicáveis apenas aos responsáveis pelos dados, enquanto os operadores de dados continuam a cumprir com as exigências de segurança de dados da lei sobre a privacidade de dados conforme disposição no Artigo 42 do anteprojeto.

COMENTÁRIOS ESPECÍFICOS

Observe que as sugestões para o novo texto estão indicadas pela cor *azul itálico* e o texto que sugerimos seja removido é indicado por ~~tachado em vermelho~~.

Escopo

Artigo 2 (II) – *Os dados pessoais relacionam-se especificamente a residentes Brasileiros caso tenham sido intencionalmente coletados no território nacional.*

Sugerimos acrescentar texto adicional para indicar que a lei se aplica apenas quando a coleta tiver intencionalmente como meta ser realizada no Brasil para evitar a confusão uma vez que a disposição atual causará imprevisibilidade. Conforme atualmente redigido, as entidades não constituídas no Brasil podem estar sujeitas à lei inesperadamente e os titulares de dados podem ficar confusos sobre se os direitos são criados quando eles se envolvem em atividades internacionais. Em algumas situações, mercadorias e serviços são oferecidos passivamente online sem uma maneira clara para determinar a localização do comprador ou do usuário final. Por exemplo, um residente do Brasil pode adquirir uma casa na Flórida e tentar obter um empréstimo bancário e seguro residencial de

um banco e de uma agência de seguros sediada na Flórida. Ou uma residente canadense pode ser titular de um cartão de crédito e ser enviada ao Brasil pelo seu trabalho. Em ambos os casos, as empresas claramente não estabeleceram as mercadorias ou serviços como "meta" para titulares dos dados no Brasil, mas podem se encontrar sujeitas à lei. Em vez de enfrentar encargos administrativos adicionais, as empresas no exemplo acima podem decidir não realizar transações com residentes do Brasil, limitando amplamente as escolhas, o acesso à tecnologia e criando um obstáculo à capacidade de participação no mercado mundial.

Além disso, deve haver isenções claras que permitam e incentivem o desenvolvimento de melhores práticas elaboradas para prevenir fraude, proteger a segurança de dispositivos, redes e instalações e atividade ilegal para permitir as obrigações existentes, tanto as legalmente exigidas quanto as voluntárias. Para simplificar, sugeriríamos incluir uma isenção adicional no Artigo 2, entretanto, concessões para essas obrigações devem ser oferecidas ao longo da proposta, inclusive em todo o Capítulo II (Artigos 7 – 15). Estas medidas incluem as disposições dos termos de serviços, códigos voluntários de boas práticas que estejam bem estabelecidos e muitos acordos internacionais. Por exemplo, as empresas de serviços financeiros precisam cumprir com vários Códigos de Prática NGO e diretrizes tais como o Código Uniforme de Prática 600 da Câmara Internacional de Comércio para atividades de financiamento de operações comerciais. A indústria de seguros também segue rigorosamente uma série de práticas padrão da indústria que, combinadas com as obrigações legais existentes em países terceiros servem para proteger os consumidores contra uma estimativa de $80 milhões *diários* em fraudes na assistência médica. O não cumprimento de tais regras, diretrizes e códigos de boas práticas podem resultar em uma ação regulatória e multas, além da diminuição da proteção de consumidores e em obstáculos para a identificação de reclamações e atividades fraudulentas.

Artigo 2(3) Parágrafo 3 É vedado aos órgãos públicos e entidades públicas efetuar a transferência de dados pessoais constantes de bases de dados que administram ou a que tenham acesso no exercício de suas competências legais para entidades privadas, exceto em casos de execução terceirizada ou mediante concessão e permissão de atividade pública que o exija e exclusivamente para fim específico e determinado.

Sugerimos incluir isenções específicas para permitir a transferência de dados pessoais para fins de bem comum, tal como emprego ou serviços de verificação de identidade, fornecimento de acesso ao crédito, gestão de riscos e prevenção contra fraudes, ameaças à segurança cibernética e outras atividades ilegais. Sugerimos também acrescentar exceções contidas no Artigo 24 para garantir a uniformidade. A Lei Brasileira de Acesso à Informação[3] pode ser usada ainda como diretriz.

[3] Vide a Lei Brasileira de Acesso à Informação (Lei 12.527/2011); Artigo 31: O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.
(3) O consentimento referido no inciso II do parágrafo 1º não será exigido quando as informações forem necessárias:
(V) - à proteção do interesse público e geral preponderante.

É importante observar que as informações registradas por autoridades e agências públicas são públicas por natureza. Desta forma, de acordo com as leis atuais do Brasil, tais informações não estariam sujeitas a qualquer restrição nesta divulgação a terceiros, exceto por motivos de segurança.

Artigo 5 Para os fins desta Lei, consideram-se as seguintes definições;

5(I) – dados pessoais: dados relacionados à pessoa natural identificada ou *razoavelmente* identificável, inclusive a partir de números identificativos, dados locacionais ou identificadores eletrônicos

Novo 5 (I)(a) *os dados pessoais não incluirão: dados não identificáveis ou anônimos.*

Conforme atualmente redigida, a definição de dados pessoais é demasiadamente ampla. Sugerimos acrescentar esclarecimentos de que dados pessoais incluam apenas dados ou conjuntos de dados tratados relativos a pessoas razoavelmente identificáveis e que não incluam dados não identificados ou tornados anônimos. Muitos tipos de dados coletados não são identificados e/ou agregados de tal maneira que seria dispendioso e demorado fazer a determinação da identidade do indivíduo. Portanto, embora tecnicamente possível, é altamente improvável que o indivíduo seja identificado. Na verdade, em algumas circunstâncias, dados adicionais precisariam ser coletados e retidos para cumprir com estas exigências do Anteprojeto de Lei. Entretanto, qualificar mais o texto do Anteprojeto servirá como incentivo para um maior uso do anonimato para os dados.

Buscamos também clareza quanto a definição de *identificadores eletrônicos*. Em particular, sugerimos acrescentar texto que especifique que esta provisão não tem a finalidade de incluir dados de pesquisa clínica tornados anônimos, dados para a prevenção contra fraudes ou atividades ilegais e não inclui registros públicos.

5(III) – dados sensíveis: dados pessoais que revelem a origem racial ou étnica, as convicções religiosas, ~~filosóficas ou morais~~, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes às *condições* de saúde ou à vida sexual, bem como dados genéticos *expressamente relacionados a um registro médico ou individual*;

Embora sejamos favoráveis à criação de diferentes categorias de dados para facilitar uma abordagem baseada em riscos para a proteção de dados, muitos dos termos nesta definição são vagos e causarão confusão. Em primeiro lugar, sugerimos eliminar a expressão "convicções filosóficas ou morais" porque o tipo de dado que se encaixa nesta categoria é, muitas vezes, bastante subjetivo. Segundo, sugerimos ainda refinar o que se quer dizer com dados referentes à "saúde". Por exemplo, deve haver uma distinção entre os dados sensíveis relativos a um exame médico comparado com uma frequência cardíaca registrada enquanto corre usando um aplicativo de corrida. Aplicativos móveis para a saúde estão tendo um crescimento exponencial e é importante garantir que os cidadãos brasileiros tenham acesso a tal tecnologia de ponta, livre de impedimentos desnecessários.

Também acrescentamos um sujestão de texto identificando que dados genéticos deveriam estar expressamente relacionados a um registro médico ou individual para incentivar a inovação e a pesquisa médica continuada. Grandes avanços médicos estão ocorrendo atualmente através do uso

de dados genéticos, que são frequentemente tornados anônimos ou totalmente aleatórios e agregados de modo a tornar os indivíduos praticamente não identificáveis.

5(IV) – dados anônimos: dados relativos a um titular, *mas a partir dos quais a identidade do titular* ~~que~~ não possa ser *razoavelmente* identificado, nem pelo responsável pelo tratamento nem por qualquer outra pessoa *com acesso ao conjunto de dados*, tendo em conta o conjunto de meios suscetíveis de serem razoavelmente utilizados para identificar o referido titular;

Nossa intenção é incentivar o anonimato dos dados sempre que for possível, indicado que apenas aqueles dados que podem ser razoavelmente identificados não seriam considerados anônimos. Isto afasta a incerteza e permite que empresas responsáveis conduzam avaliações de risco para cenários realistas, beneficiando, em particular, pequenas empresas que possuem menos recursos. Veja também nossos comentários sobre o Artigo 5(I).

Também sugerimos acrescentar uma definição e exceção para dados inúteis. Muitas vezes, mudanças na tecnologia fazem com que dados antigos fiquem inúteis e inacessíveis.

5(VII) - consentimento: manifestação livre, expressa, ~~específica~~ e informada pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada

Para incentivar a inovação e evitar custos desnecessários para as empresas, sugerimos indicar que, para dados menos sensíveis, deve haver uma norma de consentimento informado, implícito ou negativo. Comprovou-se mundialmente que, nesses casos, uma abordagem contextualizada, baseada em risco obteve sucesso.

Fornecer serviços ao consumidor através de canais digitais requer uma estrutura de consentimento flexível que permita um fluxo contínuo de dados levando em consideração o risco potencial de prejudicar o titular dos dados. Por exemplo, os dados que são licenciados por reguladores, certificados para as normas de segurança de dados e regidos por fins específicos ou limitações de uso, implicam em muito menos risco do que a transferência de dados para outras instituições sem nenhuma finalidade legítima ou específica. Portanto, o consentimento implícito ou informado do consumidor para uso e transferência de dados, em vez de ser um consentimento expresso ou afirmativo, é um padrão adequado. Tal estrutura de consentimento proporcionado deve ser implementada para evitar aumento nos custos, limites ao acesso à melhor tecnologia disponível e corte no fornecimento de serviços. Por exemplo, esta abordagem tornaria difícil aumentar de maneira eficiente os serviços financeiros para consumidores mal servidos. Para mais discussões sobre este tópico, vide nossos comentários no Capítulo II.

Além disso, as organizações necessitam proteger seus dados, propriedade intelectual, sistemas, redes de TI e outros bens contra usos fraudulentos ou ataques à segurança de computadores. Tais medidas frequentemente exigem o tratamento de dados pessoais de indivíduos, incluindo aqueles que podem estar envolvidos em atividade fraudulenta ou ataques à segurança de computadores. Obter o

consentimento nestas circunstâncias destruiria a finalidade do tratamento. Estes exemplos de tratamento poderiam também ser baseados em uma exceção de interesse legítimo.

5(XVI) - cancelamento: *um processo com a finalidade de* eliminação de dados ou conjunto de dados armazenados em banco de dados, seja qual for o procedimento empregado;

Não recomendamos definir cancelamento como um tipo de sinônimo direto para exclusão de dados. Cancelamento deve ser definido como um processo que tem como meta a exclusão /supressão de dados. Deve ser observado que pode haver motivos muito válidos, incluindo exigências legais ou regulatórias, para armazenar dados que estão sujeitos a um processo de cancelamento, embora o uso futuro de tais dados possa estar sujeito a limitações.

Artigo 6 As atividades de processamento de dados pessoais deve atender aos seguintes princípios gerais:

6(II) – princípio da adequação, pelo qual o tratamento deve ser compatível ~~com as finalidades almejadas e~~ com as *finalidades informadas ao* ~~legítimas expectativas do~~ titular, de acordo com o contexto do tratamento;

Exigir o tratamento baseado nas "finalidades almejadas" e "expectativas legítimas" do titular dos dados pode causar confusão e pode ser muito subjetivo. Portanto, sugerimos remover e acrescentar o texto adicional para aumentar a clareza.

Art 6(V) – princípio da qualidade dos dados, pelo qual devem ser garantidas a exatidão, a clareza e a atualização dos dados, *ou, nos casos onde o titular for responsável pelo fornecimento dos dados, um processo é colocado em funcionamento para permitir tais atualizações,* de acordo com a periodicidade necessária para o cumprimento da finalidade de seu tratamento;

Pode haver alguns casos onde o titular dos dados fique responsável por fornecer dados atualizados e seria inadequado ou indesejável para terceiros buscar atualizações de maneira proativa ou exigir a verificação dos dados fornecidos. Desta forma, sugerimos uma alteração no o texto para indicar que, em determinadas circunstâncias, os terceiros recebendo tais informações devem ser responsáveis por manter em funcionamento todos os processos e sistemas que possam ser necessários para permitir tal atualização.

6(IX) – princípio da não discriminação, pelo qual o tratamento não pode ser realizado para fins discriminatórios.

Sugerimos esclarecer que a não discriminação se aplica especificamente a atribuições tais como raça, religião ou etnia para evitar confusão quanto a decisões baseadas no histórico financeiro do titular.

<u>Consentimento</u>

Artigo 7 ~~O processamento de dados pessoais será permitido apenas após o consentimento livre, expresso, específico e informado do titular, exceto conforme disposto no art. 11.~~

~~**Parágrafo 1** O consentimento para o tratamento de dados pessoais não pode ser condição para o fornecimento de produto ou serviço ou para o exercício de direito, salvo em hipóteses em que os dados forem indispensáveis para a sua realização.~~

~~**Parágrafo 2** É vedado o tratamento de dados pessoais cujo consentimento tenha sido obtido mediante erro, dolo, estado de necessidade ou coação.~~

~~**Parágrafo 3** O consentimento deverá ser fornecido por escrito ou por outro meio que o certifique.~~

~~**Parágrafo 4** O consentimento deverá ser fornecido de forma destacada das demais cláusulas contratuais.~~

~~**Parágrafo 5** O consentimento deverá se referir a finalidades determinadas, sendo nulas as autorizações genéricas para o tratamento de dados pessoais.~~

Sobre o consentimento, deve haver um equilíbrio entre outorgar poderes ao indivíduo para exercer escolhas sobre sua privacidade e não sobrecarregar as políticas de privacidade com detalhes que em muitas situações possam confundir os consumidores ou fazer com que ignorem as políticas no geral. Conforme atualmente redigidas, as exigências para consentimento são restritivas e impediriam muitas práticas amplamente aceitas entre empresas e o uso de dados comerciais de praxe, aumentariam os custos para empresas e consumidores e privariam os consumidores de obter produtos e serviços desejados. Embora o consentimento seja um importante quesito para o tratamento de dados, ele não deve ser o único para o tratamento de dados.

O consentimento expresso deve estar limitado a situações onde ele é a única base para coletar e tratar dados. As disposições relativas ao consentimento, de modo geral, devem levar em consideração o contexto do tratamento de dados e permitir uma abordagem flexível para evitar confundir os consumidores com repetidas solicitações de consentimento em situações muitas vezes banais. Conforme atualmente redigido, os consumidores podem ficar sobrecarregados por solicitações de consentimento e serão, então, incapazes de distinguir entre as situações que são as mais importantes para eles. Acreditamos que a meta deste Anteprojeto de Lei não seja reduzir o entendimento dos consumidores ou sua capacidade de exercer o controle. A meta deve ser fazer com que os consumidores façam escolhas significativas com base nos casos em que o consentimento é exigido. Reduzir estes casos tornará o consentimento mais significativo.

Solicitar amplamente o consentimento expresso é problemático, porque o consentimento necessariamente será diferente, dependendo das circunstâncias, e a lei deve indicar que o método de consentimento não necessariamente será o mesmo para todas as finalidades. Em vez disso, o consentimento deve ser contextualizado; quanto mais sensível e de maior sigilo o dado, maior será a necessidade de conceder notificação e direito de escolha e aos indivíduos. Por exemplo, expressar consentimento pode ser adequado quando diz respeito à coleta de registros médicos sensíveis. Entretanto, o consentimento deve estar implícito para coleta de dados comumente aceitos e práticas

de uso, tais como um tratamento de transação solicitada pelo consumidor, gestão de riscos, segurança de dados e análise de desempenho de aplicativos e serviços.

Além disso, os consumidores serão colocados em riscos maiores uma vez que a detecção de fraude e verificação de identidade serão muito restritas. Por exemplo, as instituições financeiras podem não ser capazes de fornecer crédito e capital à crescente classe média brasileira e empresas de pequeno e médio porte do Brasil. O texto atual também restringiria sobremaneira a capacidade de fornecedores de seguro de conduzir avaliações de risco e poderiam prejudicar o crescimento econômico do Brasil. O texto a seguir simplifica a definição de consentimento, eliminando uma possível confusão para os consumidores e evitando incerteza sobre se muitos produtos e serviços sob demanda que permaneceriam legais.

O consentimento deve ser obtido através de qualquer método adequado onde os indivíduos estejam cientes que estão fornecendo seu consentimento para o tratamento de dados pessoais. Caso o consentimento do titular dos dados deva ser dado após um pedido eletrônico, tal pedido deve ser claro, conciso e não desnecessariamente confuso para o uso do serviço para o qual eles são fornecidos.

As modificações também refletem a necessidade de levar em consideração as diferenças na finalidade e contexto para a coleta de dados. A meta, fornecer informações claras aos titulares de dados, é preservada e fortalecida. Como atualmente redigida, a definição é vaga, o que poderia resultar em uma confusão entre os titulares de dados. Além disso, alguns acordos contratuais são totalmente dependentes do titular dos dados fornecer o consentimento e isolar o consentimento de outras questões que podem confundir os titulares de dados.

Parágrafo 6 ~~O consentimento pode ser revogado a qualquer momento, sem qualquer custo para o titular~~.

O titular dos dados terá o direito de retirar seu consentimento a qualquer tempo, mediante leis aplicáveis e acordos contratuais (sem prejuízo às leis existentes). A retirada do consentimento não afetará a legalidade do tratamento baseado no consentimento antes de sua retirada ou a exigência legal de reter dados históricos. Quaisquer outros benefícios ou serviços ao titular que dependerem deste consentimento ou o tratamento ou retenção de dados pode ser imediatamente interrompido mediante o processamento da solicitação.

As alterações esclarecem que, quando um contrato depender de um consentimento, os titulares de dados podem apenas retirar o consentimento de acordo com os termos do contrato, bem como determinadas leis e exigências regulatórias em vigor para garantir as proteções do consumidor que podem exigir um tratamento continuado, tal como uma prevenção à fraude. Além disso, muitos benefícios e serviços dependem do consentimento para tratamento de dados e os titulares de dados devem estar cientes de que é possível que eles não possam retirar o consentimento e manter estes benefícios ou serviços. O novo texto enfatiza este ponto para que os consumidores tomem decisões

bem fundamentadas antes de decidir por retirar o consentimento.

Novo Parágrafo: *Será presumido o consentimento no contexto de tratamento e transferência par fins legítimos de transações comerciais, incluindo, entre outros, a transferência e retenção de dados relativos ao emprego para finalidades empregatícias.*

A alteração é necessária porque, no contexto de tratamento de dados relativos a empregos, responsabilizar terceiros para a obtenção de consentimento é pouco prático, impede significativamente os modelos de negócio atuais e confunde os consumidores que podem ser forçados a interagir e fornecer consentimento a uma entidade não conhecida uma vez que os operadores geralmente não interagem diretamente com os titulares dos dados. As empresas de tratamento terceirizadas, especialmente aquelas tratando dados relativos a remunerações e empregos, enfrentariam dificuldades para determinar se o responsável obteve o consentimento explícito. O acréscimo reflete a lei do trabalho atual, onde normalmente se supõe que o empregador obteve o consentimento.

O novo texto também é acrescentado para fornecer isenções para o uso de dados para fins comerciais legítimos ao mesmo tempo em que também garante que sejam fornecidas salvaguardas legais e regulatórias aos consumidores, em relação a tais fins. Por exemplo, para casos em que as seguradoras retêm informações, dentro dos limites legais aplicáveis, sobre os consumidores, beneficiários e outros indivíduos (incluindo aqueles buscando uma cotação para seguro) por motivos legais e comerciais legítimos. Na verdade, muitas leis, amplamente seguidas como melhores práticas internacionais, reconhecem atualmente a necessidade de reter dados pessoais por um período mínimo de anos para facilitar a conformidade com a lei. Existem também exigências de determinados procedimentos legais e de prova. É importante também para os consumidores /titulares dos dados entenderem que estes dados estão sendo retidos para seu benefício, por exemplo, para evitar custos associados a comportamento fraudulento de outras pessoas. Um outro exemplo existe para setores da indústria e serviços que dependem da análise de atuários que analisam dados para empresas para fins relativos a estimativas de contribuição para aposentadoria ou seguro de grupo. A capacidade de reter os dados, que são a base do trabalho do atuário, é a única maneira de defender o produto de seu trabalho em caso de contestação formal legal das conclusões do atuário. Outro exemplo importante é o relatório de crédito, onde leis e regulamentos já preveem proteções ao consumidor, mas onde o direito de apagar dados e determinados aspectos de uma exigência de consentimento não são viáveis.

~~**Artigo 8** O titular de dados pessoais com idade entre doze e dezoito anos de idade poderá fornecer consentimento para tratamento que respeite sua condição peculiar de pessoa em desenvolvimento, ressalvada a possibilidade de revogação do consentimento pelos pais ou responsáveis legais, no seu melhor interesse.~~

Sugerimos excluir esta seção porque existe um direito geral de retirar o consentimento que cobriria situações relativas a titulares dos dados de todas as idades. Além disso, a conformidade com esta exigência demandaria a coleta de informações adicionais significativas de todos os usuários com idades entre doze e dezoito, contrariando a meta geral de minimizar a coleta de dados pessoais.

Artigo 10 Parágrafo 2 Em caso de alteração *significativa* de informação referida nos incisos I, II, III ou V do caput, o responsável deverá obter novo consentimento do titular, após destacar de forma específica o teor das alterações.

Sugerimos enfatizar que as alterações devem ser significativas. Pequenas alterações na tecnologia ou infraestrutura de organização de evento podem exigir alterações nas informações e exigir que a entidade responsável obtenha um novo consentimento para cada alteração confundirá o titular e desviará a atenção quando as alterações são verdadeiramente significativas e importantes. Isso evitaria situações que resultariam em uma sobrecarga de notificações para os consumidores.

Parágrafo 4 Nas atividades que importem em coleta continuada de dados pessoais, *além do período determinado*, o titular deverá ser informado regularmente sobre a continuidade, nos termos definidos pelo órgão competente.

Para evitar confusão e excesso de informações, sugerimos informar ao titular a coleta continuada apenas quando houver uma alteração significativa nas circunstâncias, incluindo uma alteração na duração de tempo da coleta.

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

Sugerimos esclarecer se "acesso público irrestrito" refere-se a bancos de dados públicos.

11(I) – cumprimento de obrigaçõe*s legais e, quando necessário, em relação à assinatura de um contrato*;

Para mais detalhes, consulte nossos comentários anteriores sobre o Artigo 7.

11(IV) – realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a dissociação dos dados pessoais;

O que são "pesquisa estatística?" Sugerimos uma afirmativa que esclarece que a intenção é incluir a pesquisa analítica feita para fins internos, tais como análise de compras e de mercado.

Novo 11 (VIII) *– quando o tratamento é coerente com um interesse legítimo, tal como prevenção contra fraude, outras atividades ilegais, segurança cibernética, avaliação dos riscos e outras tarefas realizadas no interesse público.*

A base do interesse legítimo para o tratamento de dados é muito importante, considerando o aumento da digitalização dos processos comerciais e sociais. Ela presta um importante papel onde pode não ser prático ou possível obter consentimento do consumidor ou onde for prematuro ou não for possível celebrar um contrato com um consumidor. Este é o caso quando a entidade responsável não tem uma relação direta com o consumidor e trata dos dados pessoais para fins

legítimos, tais como monitoramento de fraudes e para fins de prevenção. É importante ressaltar que o interesse legítimo pode ser alcançado através de um teste de equilíbrio com o objetivo de facilitar o tratamento de dados pela entidade responsável (ou por terceiros) para fins legítimos e ao mesmo tempo protegendo integralmente os direitos e interesses do consumidor. Caso o último supere o primeiro, não se pode confiar no interesse legítimo como base legal.

A exceção do interesse legítimo há muito foi incluído em muitas regras mundiais de proteção de dados, incluindo tanto a Diretriz atual da União Europeia[4] (UE), bem como incluído no novo Regulamento para Proteção de Dados Gerais da UE proposto.

Artigo 12 É vedado o tratamento de dados pessoais sensíveis, salvo

Vide comentários sobre o Artigo 5(III) relativos às preocupações sobre uma definição demasiadamente ampla de "dados sensíveis."

12 (f) tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias.

Sugerimos esclarecer o que significa "profissionais da área da saúde" e "entidades sanitárias."

Artigo 13 Parágrafo 2 O tratamento de dados pessoais biométricos será disciplinado por órgão competente, que disporá sobre hipóteses em que dados biométricos serão considerados dados pessoais sensíveis, *exceto quando usados somente e exclusivamente para fins de identificação pessoal.*

O que significa "dados pessoais biométricos?" Conforme citado em nossos comentários anteriores sobre o Artigo 5(III), gostaríamos de esclarecer que os dados clínicos tornados anônimos usados em pesquisas médicas não deveriam estar cobertos por esta definição. Além disso, os dados biométricos pessoais às vezes são necessários para identificar titulares para aumentar a segurança e proteger os consumidores e, com tal finalidade, não devem ser tratados como dados sensíveis que exigem consentimento. Desejamos reiterar nossos comentários anteriores relativos à implementação de um órgão competente e enfatizar a importância da implementação gradual da regulamentação para conformidade com quaisquer exigências adicionais conforme determinadas pelo órgão competente.

Art 14(iv)(1) Parágrafo único. Órgão competente ~~estabelecerá~~ *pode, em determinados casos,* estabelecer períodos máximos para o tratamento de dados pessoais, ressalvado o disposto em legislação específica, *ou conforme acordado em acordos contratuais.*

Sugerimos adicionar texto para permitir a continuação de acordos comerciais existentes, fornecimento continuado de serviços e melhorias na experiência do consumidor.

Existem muitos casos onde os períodos de retenção específicos, máximos ou mínimos, podem não fazer sentido. Deve-se incentivar a autoridade competente a trabalhar em conjunto com as

[4] Vide Diretriz UE 95/46/CE Artigo 7(f) que prevê: "Os Estados-Membros farão com que os dados pessoais possam ser tratados apenas caso: … (f) o tratamento seja necessário para fins de interesses legítimos buscados pelo controlador ou por terceiros a quem os dados foram divulgados, exceto onde tais interesses sejam sobrepostos pelos interesses ou direitos fundamentais e liberdades do titular dos dados que exija proteção de acordo com o Artigo 1(1)".

empresas para desenvolver políticas não vinculantes e melhores práticas que correspondam ao contexto no qual as informações são usadas e os riscos associados.

Artigo 17 O titular dos dados pessoais tem direito a obter

17(II) - acesso *razoável a dados, exceto quando tal acesso coloca em risco a privacidade e a segurança de dados pessoas relativos a outra pessoa ou durante o curso de uma pesquisa clínica onde tal acesso poderia prejudicar a integridade da pesquisa*

Para evitar confusão para o titular dos dados e criar expectativa não razoável, sugerimos acrescentar texto para clareza e criar exceções claras.

17(IV) – dissociação, bloqueio ou cancelamento de dados desnecessários ~~ou excessivos~~ ou tratados em desconformidade com o disposto nesta Lei.

Sugerimos riscar a expressão "dados excessivos" uma vez que é passível de ter uma interpretação subjetiva e supérflua após "desnecessários," gerando incerteza e confusão.

Pode haver motivos comerciais legítimos para reter dados que poderiam, de outro modo, ser considerados desnecessários ou excessivos, tais como prevenção contra fraudes ou manutenção de registro. Além disso, é muito difícil determinar quando os dados não são mais necessários, uma vez que pode ser difícil saber qual será a utilização final dos dados e se haverá necessidade futura para os mesmos.

Parágrafo 2 Os direitos previstos neste artigo serão exercidos mediante requerimento do titular a uma das ~~agentes de processamento~~ *entidades responsáveis*, que adotará ~~imediata~~ providência para seu atendimento *em até trinta dias.*

Exigir "providência imediata" seria muito oneroso. As organizações necessitam de um tempo razoável para responder e agir a tais requerimentos. Um período de tempo de 30 dias seria mais adequado. Do mesmo modo, estes requerimentos devem ser apresentados à entidade responsável em vez do agente de tratamento.

Parágrafo 3 Em caso de impossibilidade de adoção imediata da providência de que trata o Parágrafo 2, a entidade responsável enviará ao titular, *em até trinta dias* ~~em até sete dias~~ a partir da data do recebimento da comunicação, resposta em que poderá:

Sete dias é um período de tempo muito curto e causará grande pressão nos recursos, tanto do ponto de vista monetário quanto técnico. As melhores práticas gerais preveem 30 dias ou mais, tal como no México, e a mudança no texto ainda incentivará respostas imediatas ao mesmo tempo em que evitará o a sobrecarga às empresas.

Parágrafo 5 O responsável deverá informar aos terceiros a quem os dados tenham sido comunicados sobre a realização de correção, cancelamento, dissociação ou bloqueio dos dados, ~~para que repitam idêntico procedimento.~~

Seria inadequado responsabilizar uma parte para garantir uma sequência interminável de providências tomadas por terceiros com quem os dados foram compartilhados de maneira segura e legal, especialmente quando os dados são frequentemente manipulados e transformados.

Além disso, em determinadas situações onde um titular dos dados tomou medidas de maneira independente e afirmativa para tornar as informações públicas, não é razoável esperar que a entidade responsável seja capaz de identificar e rastrear todos os dados, especialmente caso algo se torne 'viral'. Não devem ser dadas aos titulares dos dados expectativas não razoáveis (e tecnologicamente impossíveis) para o limite do cancelamento e eles devem entender o verdadeiro limite até onde as informações podem ser corrigidas e desvinculadas.

Artigo 18 A confirmação de existência ou o acesso a dados pessoais *que estejam razoavelmente acessíveis no curso ordinário dos negócios, e o acesso aos quais não infrinja os direitos de outra pessoa ou comprometa informações internas,* serão providenciados, a critério (solicitação) do titular:

18(I) – em um formato simplificado, *em até trinta dias* ~~imediatamente~~; ou

18(II) – ~~por meio de declaração clara e completa, que indique a origem dos dados, data de registro, critérios utilizados e finalidade do tratamento, fornecida no prazo de até sete dias, a contarem do momento do requerimento do titular.~~

Uma vez que muitas empresas podem estar diante de milhares de solicitações, conforme atualmente redigido no Anteprojeto de Lei proposto, não será possível responder essas perguntas de maneira precisa ou efetiva em sete dias. A proposta deve evitar um período de tempo prescritivo; ao invés disso, sugerimos uma notificação sem a expressão "imediatamente."

Sugerimos ainda a exclusão do Artigo 18(II), uma vez que muitas entidades responsáveis não tratarão ou coletarão o tipo sugerido de dados. Qualquer proposta deve incentivar a coleta de menos dados, ao invés de ordenar mais solicitações de coleta, especialmente quando não está totalmente claro que benefícios aos consumidores aquelas informações podem fornecer.

Parágrafo 3 O titular poderá solicitar cópia eletrônica integral dos seus dados pessoais em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento, sempre que o banco de dados estiver em suporte eletrônico.

Primeiramente, sugerimos que seja fornecido esclarecimento que a quantidade de solicitações de um indivíduo seja limitada de modo a não criar um peso desnecessário sobre as empresas tratando os dados. Em segundo lugar, a maioria dos dados é tratada e armazenada em um formato confidencial que aumenta tanto a segurança quanto a privacidade daqueles dados. Solicitar que os dados sejam fornecidos em um formato para utilização subsequente expõe os dados a um risco maior e limita enormemente a inovação.

<u>Comunicação e Interconexão</u>

Artigo 22 Nos casos de comunicação ou interconexão de dados pessoais, o cessionário ficará sujeito às mesmas obrigações legais e regulamentares do cedente, *ou como de outro modo acordado nos acordos contratuais entre o cedente e o cessionário*. ~~com quem terá responsabilidade solidária pelos danos eventualmente causados.~~

Os cessionários normalmente não exercem qualquer supervisão ou controle operacional de cedentes; portanto, é inadequado criar uma responsabilidade solidária obrigatória para questões que podem ocorrem muito além do controle ou descoberta através de auditoria completa. As disposições sobre responsabilidade e indenização são partes principais em contratos comerciais. O Artigo 22 como está redigido seria problemático para relações duradouras. Esta exigencia é especialmente problemática em casos onde uma entidade excepcionalmente grande deseja contratar uma empresa pequena para realizar atividades de tratamento. Embora seja totalmente realista impor a uma empresa de pequeno porte as mesmas normas de proteção de dados, é totalmente inadequado esperar que uma empresa de pequeno porte possa sofrer as mesmas penalidades em potencial que uma grande empresa multinacional. A responsabilidade solidária obrigatória desencorajará o desenvolvimento de empresas *startup* e empreendedorismo.

Acreditamos que deve ser permitido pela lei às entidades responsáveis que aloquem contratualmente suas respectivas responsabilidades, refletindo, desse modo, seus respectivos papéis e relações diretas ou indiretas com os titulares dos dados. Alguns tipos de atividades de tratamento podem não necessariamente resultar em uma relação direta com o titular e as empresas teriam que coletar informações adicionais sobre o titular, o que se opõe ao princípio de minimização de dados. A responsabilidade solidária deveria deste modo, aplicar-se apenas a entidades de responsabilidade solidária quando não determinarem suas responsabilidades e obrigações em um acordo por escrito.

Artigo 23 A comunicação ou interconexão de dados pessoais entre pessoas de direito privado dependerá de consentimento livre, expresso, específico e informado, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

Sugerimos esclarecer que existe uma isenção para funções técnicas, tal como quando uma entidade responsável transfere sistemas operacionais ou se muda para um novo local de hospedagem para computação em nuvem.

<u>Transferência Internacional de Dados</u>

Artigo 28 A transferência internacional de dados pessoais somente é permitida para países que proporcionem nível de proteção de dados pessoais equiparáveis ao desta Lei, ressalvadas as seguintes exceções:

28(I) – quando a transferência for necessária para a cooperação judicial internacional entre órgãos públicos de inteligência e de investigação, de acordo com os instrumentos de direito internacional;

28(II) – quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

28(III) – quando órgão competente autorizar a transferência, nos termos de regulamento;

28(IV) – quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

28(V) – quando a transferência for necessária para execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do Parágrafo 1 do art. 6.

Novo Artigo 28(VI) *– quando a transferência é necessária para cumprir com obrigações legais e de outro modo cumprir com acordos contratuais;*

Novo Artigo 28 (VII) *– quando a transferência é de interesse público ou interesse legítimo, tal como prevenção contra fraudes, proteção à segurança de computadores e atividade de avaliação de riscos;*

Novo Artigo (VIII) *– quando a transferência é necessária no contexto de trabalho, atividade de recursos humanos e processos internos na empresa;*

Novo Artigo 28(IX) *- quando o titular forneceu anteriormente seu consentimento para a entidade responsável permitindo que esta realizasse a transferência para um país que não pode fornecer o mesmo nível de proteção pessoal que o Brasil.*

Conceitos de "adequação" são frequentemente problemáticos, inconsistentes e impedem a inovação. Estima-se que as restrições sobre as transferências de dados além-fronteiras no Brasil resulte em um prejuízo de 0,8% ao PIB e uma diminuição de 4,2% em investimentos.[5]

É importante observar que as regras de proteção de dados seguem junto com os dados para onde quer que estes sejam transferidos e as entidades responsáveis pela transferência devem ser capazes de avaliar como melhor garantir que aquelas proteções sejam alcançadas de uma maneira eficaz em termos de custos. Entretanto, sugerimos aqui várias exceções adicionais que acreditamos necessárias para assegurar que as empresas e consumidores brasileiros possam participar e prosperar no mercado mundial.

Apoiamos fortemente as exceções para o conceito de "acordos de cooperação internacional" e gostaríamos de esclarecer que a intenção é cobrir acordos, tais como o Sistema de Regras de Privacidade entre Fronteiras da APEC (CBPR) e as melhores práticas setoriais internacionalmente reconhecidas. Caso contrário, sugerimos acrescentar texto para cobrir tais acordos.

Parágrafo Único. O nível de proteção de dados do país será avaliado por órgão competente, que levará em conta:

I – normas gerais e setoriais da legislação em vigor no país de destino*, incluindo aquelas em níveis sub-federais*;

5 O Impacto Econômico do Marco Civil da Internet no Brasil, Bert Verschelde, European Centre for International Political Economy (ECIPE), maio de 2014, disponível no endereço http://www.ecipe.org/app/uploads/2014/12/ECIPE_bulletin614_dataloc_brazil.pdf.

II – a natureza dos dados;

III – observância dos princípios gerais de proteção de dados pessoais previstos nesta Lei;

IV – adoção de medidas de segurança previstas em regulamentos; e

V – outras circunstâncias específicas relativas à transferência.

Novo VI – *confiabilidade e uniformidade do cumprimento no país de destino.*

Novo Parágrafo – *A avaliação por órgão competente será realizada de maneira oportuna, transparente e fundamentada.*

Em caso de descoberta não equivalente, (i) o argumento será totalmente explicado; (ii) será outorgada à autoridade competente a capacidade de permitir transferências relativas a setores específicos ou tipos e usos de dados; e (iii) será reavaliada tal descoberta mediante notificação por país ou parte interessada de uma atualização às normas de proteção de dados.

Desejamos observar que uma "autoridade competente" é responsável por avaliar o nível de proteção de dados de outros países. Isto é particularmente problemático, uma vez que atualmente não está claro quando a autoridade competente será indicada ou por quanto tempo tal entidade precisaria estar totalmente funcional. Seria necessário mais tempo para avaliar os níveis de proteção de dados de outros países, criando uma incerteza permanente. Portanto, caso o Artigo 28 permaneça no texto, sugerimos fornecer orientação esclarecendo que mecanismos de transferência de dados e melhores práticas em vigor no momento da aprovação do Anteprojeto de Lei permaneçerão válidos até que tais determinações possam ser efetuadas.

Além disso, é fundamental que qualquer autoridade competente atue de maneira transparente e oportuna. Sugerimos também a criação de diretrizes que exijam a coleta de informações da parte interessada para criar uma avaliação totalmente informada.

Outras leis gerais de proteção de dados em países da América Latina preveem permitir as transferências internacionais de dados para países que não podem fornecer o mesmo nível de proteção, através da obtenção de consentimento do titular autorizando a entidade responsável a realizar tal transferência internacional. Isso inclui leis gerais de proteção de dados do México, Peru e Colômbia, entre outros. Acreditamos que essa possa ser uma solução razoável e prática.

Artigo 29. Nos casos de países que não proporcionem nível de proteção equiparável ao desta Lei, o consentimento de que trata o art. 7 será especial, fornecido:

29(I) – mediante manifestação própria, ~~distinta da manifestação de consentimento relativa a outras operações de tratamento~~; e – assinatura digital?

29(II) - com informação prévia e específica sobre o caráter internacional da operação, com alerta quanto aos riscos envolvidos, de acordo com as circunstâncias de vulnerabilidade do país de destino.

Desejamos oferecer concordância com o uso do consentimento como um possível mecanismo de transferência de dados, quando exceções, incluindo nossas exceções propostas, não estão disponíveis. É importante informar aos titulares dos dados de riscos em potencial para deixar que eles tomem decisões informadas. Isso concede poderes aos titulares dos dados em vez de sujeitar todas as decisões a uma abordagem excessivamente prescritiva, de cima para baixo.

Sugerimos que o texto do Artigo 29(1) seja excluído, uma vez que exigir múltiplos casos de consentimento resulta em confusão para os titulares dos dados. Com isso, notificações verdadeiramente importantes poderão passar despercebidas.

Artigo 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 pelo exportador dos dados e pela entidade responsável pelo tratamento, bem como* ~~aprovadas para uma transferência específica~~, em cláusulas contratuais-padrão ou em normas corporativas globais, nos termos do regulamento.

As mudanças sugeridas eliminam a redundância e simplificam a conformidade.

Parágrafo 1 O 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~~.

Embora as cláusulas contratuais padrão possam ser úteis, é importante que não sejam consideradas o único método para criar mecanismos para transferência de dados. Além disso, tais cláusulas padrão devem permitir que as partes em contratos comerciais cheguem a um acordo quanto à responsabilidade, desde que as responsabilidades sejam totalmente detalhados, uma vez que em muitos acordos de transferência exigir a responsabilidade solidária é inadequado, especialmente quando uma das partes é muito maior. Consulte nossos comentários anteriores relativos à responsabilidade solidária para obter mais informações.

Parágrafo 2 As entidades 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.

Parágrafo 3 *Caso sejam feitas alterações à cláusula contratual padrão ou normas corporativas mundiais* ~~Na análise de cláusulas contratuais ou de normas corporativas globais submetidas à aprovação de órgão competente~~, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento.

Entendemos de acordo com o Parágrafo 3 que as empresas precisam obter aprovação das cláusulas padrão de uma autoridade competente, o que seria muito trabalhoso tanto para as empresas quanto

para os reguladores. Isso criaria grandes acúmulos, uma vez que a autoridade seria inundada por solicitações para aprovação, criando um consumo desnecessário de recursos da autoridade competente e atrasando a implementação das cláusulas contratuais que são amplamente aceitas mundialmente. Em vez disso, recomendamos habilitar a aprovação automática das cláusulas contratuais padrão adotadas pelo cedente e cessionário e apenas buscar informações adicionais em caso de alterações.

Artigo 31. ~~O cedente e o cessionário têm responsabilidade solidária pelo tratamento de dados realizado no exterior ou no território nacional, em qualquer hipótese, independente de culpa.~~

Pedimos consultar comentários anteriores sobre responsabilidade solidária.

Artigo 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.

Solicitamos esclarecer que a referência a "normas" neste Artigo refere-se a exigências legais e regulatórias em vigor no território de coleta.

Artigo 35. Todo aquele que, por meio do tratamento de dados pessoais, *infringindo estas regras*, causar a outrem dano material ~~ou moral~~ individual ou coletivo, é obrigado a ressarci-lo.

Sugerimos limitar danos a situações onde os titulares dos dados possam demonstrar danos materiais. Permitir reivindicações com base em danos "morais" criará um grande número potencial de reivindicações impraticáveis, muitas delas baseadas em argumentação subjetiva. Isso poderia resultar em desviar o sistema judiciário brasileiro de casos verdadeiramente prioritários, atrasando a capacidade daqueles verdadeiramente prejudicados de seu direito a uma audiência.

Também adicionamos um texto esclarecedor para indicar que o processamento deve ocorrer no local da infração da lei, uma vez que em alguns casos, especialmente aqueles relativos a decisões financeiras quando um titular dos dados pode sofrer "danos materiais", mas os dados teriam sido totalmente protegidos e tratados de acordo com a lei. Por exemplo, um residente brasileiro pode ter um longo histórico de não pagar empréstimos ou hipotecas. Após uma análise do histórico de crédito, um banco decide, de forma legítima, não conceder outro empréstimo àquele residente, resultando na retomada de posse de um automóvel. Esta decisão poderia, possivelmente, ser considerada como causadora de danos materiais, mas ela é totalmente justificável.

Parágrafo 2 O responsável ou o operador podem deixar de serem responsabilizados se provarem que o fato que causou o dano não lhes é imputável.

Embora o texto tenha o nosso apoio, buscamos esclarecimento sobre como isso interagiria com outros textos relativos à responsabilidade solidária obrigatória.

Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pela entidade *responsável* ~~pelo tratamento~~, que verificará a observância das próprias instruções e das normas sobre a matéria.

~~**Parágrafo 1** O responsável tem responsabilidade solidária quanto a todas as operações de tratamento realizadas pelo operador.~~

Recomendamos alterações ao Artigo 39, incluindo a exclusão do Parágrafo 1, porque a responsabilidade deve ser atribuída apenas à entidade responsável. A entidade responsável dá instruções ao operador de dados através de um acordo contratual e caso o operador não aja de acordo com as instruções, o operador será responsabilizado perante a entidade responsável pela aplicação das cláusulas de responsabilidade contratual que foram acordadas entre eles.

Encarregado pelo Tratamento de Dados Pessoais

Artigo 41 O responsável deverá indicar um *ponto de contato para questionamentos ou preocupações relativos à implementação destas disposições.* ~~encarregado pelo tratamento de dados pessoais.~~

Parágrafo 1 A identidade e as informações de contato do encarregado devem ser ~~publicamente~~ *conhecidas dentro da entidade responsável, e o ponto de contato para o escritório de proteção de dados da entidade responsável (mas não necessariamente o nome da pessoa encarregada) serão* divulgadas de forma clara e objetiva, preferencialmente na página eletrônica do responsável na Internet.

Sugerimos remover as exigências de indicar uma única pessoa como ponto de contato para toda a organização, uma vez que a organização interna e as responsabilidades do cargo tornam as exigências de um contato específico ineficientes. Para grandes empresas, um único ponto criaria um gargalo, atrasando respostas e enfraquecendo comunicados de boas vindas. E pequenas empresas normalmente não têm recursos para alocar uma única pessoa para um cargo em tempo integral.

Artigo 44. A entidade responsável deve ~~imediatamente~~ comunicar ao órgão competente a ocorrência de qualquer incidente de segurança que possa acarretar prejuízo *significativo* aos titulares *sem demora excessiva.*

Artigo 45. O órgão competente poderá determinar a adoção de providências quanto a incidentes de segurança relacionados a dados pessoais, conforme sua gravidade, tais como:

45(I) – ~~pronta comunicação aos titulares;~~

45(II) – ampla divulgação do fato em meios de comunicação; ou

45(III) – medidas para reverter ou mitigar os efeitos de prejuízo.

Parágrafo 1 No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas
medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis para terceiros não autorizados a acessá-los.

Parágrafo 2 ~~Pronta~~ comunicação aos titulares afetados pelo incidente de segurança será obrigatória~~, independente de determinação do órgão competente,~~ nos casos em que for possível identificar que o incidente ~~coloque em risco~~ *tenha uma possibilidade razoável de i) colocar em risco* a segurança pessoal dos titulares ou *ii) criar um risco de dano material ao titular* ~~ou lhes possa causar danos~~.

Embora acreditemos que os critérios para comunicações em relação à violação de dados sejam essenciais, conforme atualmente redigido no Anteprojeto de Lei proposto, não será possível responder "prontamente" estas questões de modo preciso ou eficiente. Esta exigência de uma pronta resposta mudará, em última análise, o foco das responsabilidades administrativas e de comunicação em vez de abrir uma brecha para a mitigação. Leva tempo para avaliar-se a natureza e escopo de uma violação e se a violação pode causar danos aos titulares dos dados. Embora seja importante notificar consumidores impactados oportunamente, é mais importante que a notificação apresente os fatos da violação de maneira completa e precisa.

O Anteprojeto de Lei deveria evitar um período de tempo prescritivo; ao invés disso, sugerimos que uma notificação seja enviada sem demora desnecessária. As alterações oferecem flexibilidade e canalizam a prioridade no sentido de garantir a proteção dos dados em vez de cumprir com exigências administrativas trabalhosas. As alterações também ajudam a evitar um ambiente onde os consumidores possam ser bombardeados com notificações e que aquelas notificações verdadeiramente importantes se percam no meio de tantas outras. Também sugeriríamos adicionar uma definição para uma violação significativa ou grave para ajudar a preservar os recursos da autoridade supervisora. Além disso, esta alteração evitará sobrecarregar a autoridade competente com notificações constantes; o que tornaria difícil concentrar os recursos e a atenção quando ocorrerem violações significativas.

Artigo 50 As infrações realizadas por pessoas jurídicas de direito privado às normas previstas nesta Lei ficam sujeitas às seguintes sanções administrativas aplicáveis por órgão competente:

50(I) – multa simples ou diária;

50(II) – publicação da infração;

50(III) - dissociação dos dados pessoais;

50(IV) – bloqueio dos dados pessoais;

50(V) - suspensão de operação de tratamento de dados pessoais, por prazo não superior a dois anos;

50(VI) - cancelamento dos dados pessoais;

50(VII) – proibição do tratamento de dados sensíveis, por prazo não superior a dez anos; e

Apoiamos ideias para permitir uma escala flexível de multas a serem aplicadas de acordo com a extensão e duração da infração. Apreciaríamos esclarecimentos sobre o que significa uma "multa

simples," ao mesmo tempo em que também enfatizamos que o Brasil deveria evitar quaisquer alterações que levaria a enumerar porcentagens específicas.

As multas previstas no Artigo 50(V), (VI), e (VII) podem, de fato, fechar uma empresa ou, no mínimo, forçar a empresa a sair do mercado brasileiro, privando os residentes brasileiros de escolhas e serviços valiosos. Devido ao fato desta multa ser claramente criada apenas para os piores infratores, sugerimos, como alternativa, exigir um período de maior supervisão e conformidade. Do mesmo modo, impor estas medidas para limitar serviços e conteúdo como medida punitiva sem as diretrizes estabelecidas que limitariam a sua aplicação ou implementação, faz surgir preocupações sobre se elas poderiam estar contrariando os interesses da liberdade de expressão e, conforme observado no Marco Civil da Internet, vir contra toda a disciplina sobre o uso da Internet no Brasil que está fundamentada na base do respeito pela liberdade de expressão.

Artigo 51. O órgão competente estabelecerá normas sobre adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, considerada a complexidade das operações de tratamento, a natureza dos dados e o porte do responsável.

Não está claro para nós a finalidade deste Artigo e gostaríamos que mais detalhes fossem dados em relação à sua intenção. Sugerimos evitar qualquer uso de normas obrigatórias, formatos e tecnologias e, em vez disso, exigir o uso das melhores práticas internacionais amplamente aceitas. Isso evitaria trabalho administrativo desnecessário e garantiria que as empresas pudessem utilizar práticas de proteção de dados de vanguarda. Além disso, exigir tecnologia específica resultaria em inalterabilidade de bancos de dados desatualizados e possivelmente inseguros.

Queremos reiterar a necessidade da autoridade competente de definir normas de uma maneira transparente que permita tempo para consultas significativas as partes interessadas. Isso permitiria que a autoridade alavanque as melhores práticas existentes, garantiria que quaisquer propostas refletissem as realidades técnicas e comerciais e evitaria incerteza legal.

Em relação aos dados contidos nos bancos de dados que já estavam em vigor no momento da aprovação da lei, eles deveriam respeitar o princípio jurídico da lei jurídica perfeita, de acordo com a qual tais leis não podem estar sujeitas à nova legislação conforme baseado no Art. 6º da Lei Introdutória ao Código Civil Brasileiro.

Artigo 52. Esta Lei entrará em vigor ~~em~~ *pelo menos um ano* ~~120 (cento e vinte) dias contados da sua data de publicação~~ *após o estabelecimento de uma autoridade competente independente, totalmente operacional, financiada de modo sustentável e equipada com funcionários, e depois que tal autoridade emitir quaisquer outras regras ou exigências necessárias.*

Observamos que muitas disposições desta lei dependem ainda de esclarecimentos da autoridade competente, que ainda não existe. As empresas precisarão de tempo adequado para criar alterações necessárias para garantir a conformidade com esta regra e será impossível saber que alterações podem ser necessárias até que a autoridade competente forneça mais orientações. Empresas de

pequeno e médio porte enfrentariam um fardo ainda maior, uma vez que as alterações necessárias poderiam, frequentemente, custar centenas de milhares de dólares e muitas horas de trabalho.

Além disso, algumas disposições, tais como aquelas relativas a transferências de dados, podem depender de uma aprovação da autoridade competente. Caso a lei entre em vigor antes da existência desta autoridade, as empresas enfrentarão uma escolha impossível entre infringir a lei ou construir um muro artificial em volta do Brasil ou retirar-se do comércio mundial. Os consumidores também poderão se ver sem acesso a produtos e serviços valiosos.

Portanto, nossas sugestões de edição foram elaboradas para criar uma data de implementação após a criação da autoridade competente e também fornecendo tempo adequado para que as empresas façam quaisquer alterações necessárias.