PL 5276/2016 (proteção de dados) - Nota Técnica

Sumário

***

Introdução

O Brasil se encontra na posição única de elaborar uma lei que fortaleça e promova a proteção de dados pessoais e a inovação, de maneira convergente e não contraditória.

Desde o início da sua elaboração em 2010 até o texto enviado ao Congresso, este projeto de lei evoluiu em vários pontos. São excelentes exemplos nesse sentido o reconhecimento da liberdade de expressão, de comunicação e de opinião, do desenvolvimento econômico e tecnológico, da livre iniciativa e da livre concorrência, de forma convergente com a defesa do consumidor, como fundamentos da disciplina da proteção de dados (art. 2º), o reconhecimento dos interesses legítimos do responsável como uma das bases para o tratamento dos dados (art. 7º, IX) e a valorização à adoção de regras de boas práticas organizacionais (art. 50).

Apesar desses importantes avanços, ainda são necessários alguns ajustes ao texto do projeto de lei a fim de que ele se alinhe ainda mais com a função social e o impacto econômico que a legislação sobre proteção de dados pessoais virá a ocupar no ordenamento brasileiro. O Brasil pode e deve encontrar seu modelo próprio, que coloque o país em posição de liderança na proteção de dados pessoais e na promoção da inovação na região latino-americana e além dela - e, mais do que isso, que atenda às necessidades e especificidades do país sem a tentação de copiar modelos menos vanguardistas e que ainda não tenham sido testados com êxito.

Uma lei de proteção de dados comprometida com a promoção da inovação e com o dinamismo da economia e da sociedade baseada em dados deve conter conceitos claros e diretos, que possam ser facilmente compreendidos e aplicados, e deve adotar uma abordagem baseada em princípios e na neutralidade tecnológica como forma de se manter relevante e viva com o passar do tempo, sem a prescrição de regras adstritas a tecnologias que existem hoje e podem deixar de existir amanhã. Deve ainda, como comentaremos em maior detalhe a seguir, prever uma gama suficientemente ampla de bases legais para o tratamento e a transferência de dados, sem deixar de garantir as salvaguardas, a proteção e a experiência fluida e informada (*user experience* ou UX) dos titulares de dados nesses processos. Para tanto, a lei deve prever diversos fundamentos legais para tratamento de dados, que vão do consentimento inequívoco ao legítimo interesse, e que possam - cada uma delas - aplicar-se de forma pragmática e contextual, permitindo, a um só tempo, uma ampla gama de usos benéficos dos dados na era da informação e a proteção dos indivíduos titulares dos dados. A lei deve também prever um amplo leque de bases legais válidas para as transferências internacionais de dados, que reflitam e sejam capazes de dialogar com todos os outros mecanismos de transferências internacionais em vigor, permitindo assim o fluxo de dados, que é primordial tanto para a economia moderna como para o progresso da sociedade.

Listamos e comentamos abaixo seis pontos prioritários do PL que podem ser aprimorados nesse sentido.

1. [art. 5º, I e art. 13, §1º] A definição de dados pessoais deve ser menos ampla e os dados anonimizados devem ser claramente excluídos do escopo da lei

O PL 5276 caracteriza como dado pessoal qualquer "dado relacionado a pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa". A definição é excessivamente ampla e exemplificativa, trazendo questionamentos adicionais àqueles que tratam as espécies de dados exemplificadas na definição e muito possivelmente inibindo que novas empresas e novos modelos de uso de tais dados para fins sociais e/ou econômicos se desenvolvam no país.

Ao se pensar na definição de "dados pessoais" é preciso lembrar que nem todas as informações "referentes a" uma pessoa são criadas e tratadas da mesma maneira ou têm o mesmo valor para todos responsáveis ou operadores (nos termos do art. 3º, VI e VII). Mais do que buscar uma definição ampla e proibitiva de dados pessoais, o incentivo legal a programas de cumprimento da lei (*accountability*) — como o PLS 330 de forma bastante vanguardista ensaiou em seu art. 50 — tem demonstrado um efeito prático muito mais significativo e eficaz, e já é uma realidade em países como o México e a Colômbia, por exemplo.

O critério para definir dado pessoal deveria estar atrelado ao potencial de tal dado efetivamente identificar uma pessoa determinada, podendo afetar a sua privacidade. Nos Estados Unidos, por exemplo, o conceito de "informação pessoalmente identificável" (*personally identifiable information* ou PII) é usado largamente e parte da correlação entre um dado e a identificação de uma pessoa determinada. A lei de Singapura, por sua vez, também oferece um exemplo intermediário de definição de dados pessoais como uma informação sobre um indivíduo que "pode ser identificado a partir daqueles dados" ou de outros dados a que uma organização possa razoavelmente ter acesso.

Nem todo dado meramente "relacionado a" uma pessoa carrega o potencial de identificar tal pessoa. Por exemplo, a informação de que uma pessoa gosta de esportes ou de literatura pode ser considerado um dado "relacionado a" uma pessoa, porém, isoladamente, esse tipo de informação é incapaz de efetivamente identificar uma pessoa natural ou de afetar de qualquer modo a sua privacidade, e, portanto, não deveria ser considerado um dado pessoal. Justamente por isso é que os dados anônimos e anonimizados — assim entendidos os dados relativos a um titular que não possa ser identificado, conforme o art. 5º, IV do PL 5276 — devem ser claramente retirados do âmbito de aplicação da lei, conforme o modelo adotado no PLS 330, por exemplo, em seu art. 2º, §3º, IV.

Assim, em consonância com outros projetos de lei sobre proteção de dados pessoais em tramitação na Casa, como o PL 4060/2012, sugerimos emenda ao inciso I do art. 5º de modo que a definição de dado pessoal seja a seguinte:

I - <u>dado pessoal: qualquer informação que permita a identificação precisa de uma pessoa</u>;

Pelos mesmos motivos, sugerimos a exclusão do §1º do art. 13:

~~**§ 1º Poderão ser igualmente considerados como dados pessoais para os fins desta Lei os dados utilizados para a formação do perfil comportamental de uma determinada pessoa natural, ainda que não identificada.**~~

Além disso, embora o PL 5276 tenha caminhado bem ao definir os chamados dados anonimizados (art. 5º, IV) e estabelecer linhas gerais sobre o seu regime (art. 13), ele não foi claro o suficiente sobre a exclusão dessa categoria de dados do âmbito de aplicação da lei ou sobre os incentivos da desanonimização — o PLS 330, por exemplo, foi muito mais didático nesse sentido. Estimular a anonimização dos dados por todos aqueles submetidos à lei (sejam pessoas naturais ou jurídicas, de direito público ou privado), conforme, por exemplo, a diretriz do §4º do art. 11 do projeto, é uma forma bastante efetiva de proteger o direito à liberdade e à privacidade dos titulares que a lei pretender resguardar, segundo seu art. 1º. Para promover esse incentivo, em vez de prever mecanismos executivos, como o disposto no §3º do art. 13, o projeto deveria ser mais explícito quanto à possibilidade de considerar anônimos não só os dados que não possam ser revertidos "com esforços razoáveis", mas também aqueles cujo tratamento se baseie em obrigação contratual, administrativa ou legal de anonimização.

Por esses motivos, sugerimos os seguintes ajustes aos arts. 4º e 13 do PL 5276:

Art. 4º. Esta lei não se aplica ao tratamento de dados:

I - realizado por pessoa natural para fins exclusivamente pessoais;

II - realizado para fins exclusivamente jornalísticos, artísticos, literários ou acadêmicos;

III - realizado para fins exclusivos de segurança pública, de defesa nacional, de segurança do Estado ou de atividades de investigação e repressão de infrações penais; **<u>ou</u>**

<u>IV - anonimizados, desde que não seja razoavelmente possível identificar o titular ou que os responsáveis pelo tratamento estejam sob obrigação contratual, administrativa ou legal de manter os dados anonimizados.</u>

Art. 13. Os dados anonimizados serão considerados dados pessoais, para os fins desta Lei, quando o processo de anonimização ao qual foram submetidos for revertido, ou quando, com esforços razoáveis, puder ser revertido.

§1º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, dados utilizados para a formação do perfil comportamental de uma determinada pessoa natural, ~~**ainda que não identificada**~~ **desde que permitam a sua identificação precisa.**

§2º O órgão competente poderá dispor sobre padrões e técnicas utilizadas em processos de anonimização e realizar verificações acerca da sua segurança, **respeitada a livre iniciativa e os segredos de negócio;**

§3º O compartilhamento e o uso que se faz dos dados anonimizados deve ser objeto de publicidade e de transparência, **respeitada a livre iniciativa e o segredo de negócio,** sem prejuízo do órgão competente poder solicitar ao responsável relatório de impacto à privacidade referente aos riscos de reversão do processo de anonimização e demais aspectos de seu tratamento.

2. [art. 5º, III e art. 11] Devem ser previstas exceções claras às formalidades para o tratamento de dados sensíveis, em especial quando o seu tratamento for voltado a trazer benefícios aos titulares ou quando os titulares houverem voluntariamente disponibilizado os dados

O PL 5276 caracteriza como dados sensíveis os "dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, bem como dados genéticos ou biométricos", e exige, em seu art. 11, requisitos mais formais para o seu tratamento, especialmente consentimento expresso e em separado.

Assim como a definição de dados pessoais, a de dados sensíveis é demasiadamente ampla e não prevê qualquer tipo de parâmetro ou avaliação de risco para sua caracterização, trazendo questionamentos adicionais àqueles que tratam as espécies de dados exemplificadas na definição, e muito possivelmente inibindo no país a exploração de tais dados para fins positivos e desejáveis.

Um exemplo de tecnologia que poderia ser inibida no país é a do assistente virtual capaz de notificar as pessoas quando estiverem prestes a compartilhar imagens sensíveis online, sejam fotos ou imagens de documentos sensíveis, como dados fiscais ou cartões de crédito (http://www.vocativ.com/418862/ai-privacy-

assistants-expose-sensitive-info/). Isto é, uma tecnologia que se baseia no tratamento de dados sensíveis para proteger as pessoas quanto à sua exposição. Um outro exemplo do uso social e positivo de dados que poderiam estar abarcados por tal definição ampla de dados sensíveis e que poderia ser inibido no país é o uso de *big data* para compreender e traçar estratégias efetivas em questões de saúde pública da maior relevância - por exemplo, no caso de epidemias atingindo grandes áreas geográficas, como o Ebola ou o Zika, além do caso de sucesso do "Robô Laura", recentemente apresentado na Comissão de Seguridade Social e Família desta Casa, que permitiu uma redução drástica no número de mortes decorrentes de infecção hospitalar no Hospital Nossa Senhora das Graças, em Curitiba, garças ao uso e ao processamento inteligente de dados (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).

Graças à possibilidade de tratar tais dados referentes à saúde de modo flexível e responsável é que se pode, por exemplo, ajudar organizações não-governamentais a fazer as informações adequadas sobre prevenção e tratamento chegarem às pessoas certas, nos focos das epidemias, ajudando-as a proteger suas famílias e comunidades. Por último, caso se levassem ao extremo os requisitos para o uso de dados sensíveis, jamais poderíamos ter lido sobre o caso recente de duas crianças de 4 anos de idade que salvaram a vida da mãe que estava desacordada ao usar as digitais dela (dados biométricos) para acionar a assistente virtual Siri de seu celular e chamar a central de segurança de seu país (http://www.huffingtonpost.co.uk/entry/twins-4-use-iphone-assistant-siri-to-save-unconscious-mothers-life_uk_58d5049ce4b03692bea47ac0).

Dada a dificuldade de regulamentar, na lei geral de proteção de dados, a questão dos dados considerados sensíveis sem inibir os seus usos positivos, diversos países fizeram a opção legislativa de não abordar o tema em seus diplomas gerais sobre proteção de dados — é o caso, por exemplo, do Canadá, de Singapura e de Hong Kong. Assim, mesmo que lei brasileira, diferentemente desses países, decida disciplinar a categoria de "dados sensíveis", é preciso cuidar para que os requisitos e o consentimento para o tratamento desses dados não sejam proibitivos a ponto de, na prática, inviabilizar no país o uso benéfico desses dados, com as salvaguardas apropriadas. Além disso, a lista de dados sensíveis no inciso II do art. 3º deve ser claramente fechada, e não exemplificativa ou aberta a interpretações expansivas, que podem minar a inovação. A propósito, um estudo recente da PricewaterhouseCoopers (PwC) demonstrou como as pessoas reconhecem o valor do compartilhamento de dados sensíveis para fins positivos: por exemplo, 57% responderam que compartilhariam seus dados para ajudar no desenvolvimento de avanços na medicina, e 62%, que compartilhariam seus dados para ajudar na elaboração de soluções para aliviar o trânsito em suas cidades (http://www.pwc.com/us/en/industry/entertainment-media/publications/consumer-intelligence-series/assets/pwc-botme-booklet.pdf). Idealmente, a lei deveria reconhecer de forma clara os usos benéficos dos dados considerados sensíveis (pense-se nos avanços da área de saúde e médica nesse sentido, apenas como um exemplo mais marcante), e garantir que o Brasil

poderá continuar sendo palco desses avanços, graças à possibilidade de tratar dados sensíveis de acordo com salvaguardas protetivas e diversas bases legais para o tratamento desses dados. O art. 11 do PL 5276 inicia um bom caminho neste sentido, mas, conforme as sugestões a seguir, ainda pode dar mais espaço ao tratamento benéfico e responsável dos dados sensíveis.

A lei de proteção de dados da África do Sul, por exemplo, traça uma série de exceções à proibição do tratamento de dados sensíveis, incluindo os casos em que "a obtenção do consentimento pareça impossível ou implique um esforço desproporcional", a finalidade do tratamento seja "de interesse público e o tratamento seja necessário à finalidade em questão", "sejam asseguradas garantias suficientes para assegurar que o tratamento não prejudique de forma desproporcional a privacidade do indivíduo em causa", e "as informações tenham sido deliberadamente tornadas públicas pela pessoa em causa", além de diversas outras exceções razoáveis e flexíveis, que ademais protegem os titulares dos dados.

Ao lado disso e especificamente quando se trata de dados sociais referentes à orientação religiosa, política ou sexual, ou à convicção filosófica, à procedência nacional, à origem racial ou étnica, ou ainda à participação em movimentos políticos e sociais, é preciso ter muita cautela para não inibir a sua livre manifestação, conforme assegurado pela Constituição, nos termos do art. 5º (incisos VI, VIII e IX) dentre outros dispositivos, de forma que a lei de proteção de dados deve reconhecer e respeitar a expressão de tais convicções quando forem espontânea e livremente fornecidas pelos titulares como manifestação de sua liberdade de expressão, consciência ou crença, que constituem a base do ativismo e exercício pleno da cidadania.

Com base nisso, sugerimos que a redação do inciso III do art. 5º e do art. 11 seja emendada como se segue:

> **Art. 11.** É vedado o tratamento de dados pessoais sensíveis, exceto:
>
> I - com fornecimento de consentimento livre, inequívoco, informado, expresso e específico pelo titular;
>
> a) mediante manifestação própria, distinta da manifestação de consentimento relativa a outros dados pessoais;
>
> b) com informação prévia e específica sobre a natureza sensível dos dados a serem tratados, com alerta quanto aos riscos **e benefícios** envolvidos em seu tratamento.
>
> II - sem fornecimento de consentimento do titular, nas hipóteses **dos incisos II a IV e VI a IX do art. 7º, ou quando o titular ou seu representante legal não tiverem voluntariamente disponibilizado os dados, como**

manifestação de sua liberdade de expressão, consciência ou crença. ~~**em que for indispensável para:**~~

~~**a) cumprimento de uma obrigação legal pelo responsável;**~~

~~**b) tratamento e uso compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;**~~

~~**c) realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;**~~

~~**d) exercício regular de direitos em processo judicial ou administrativo;**~~

~~**e) proteção da vida ou da incolumidade física do titular ou de terceiro; ou**~~

~~**f) tutela da saúde, com procedimento realizado por profissionais da área de saúde ou por entidades sanitárias.**~~

§1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais capaz de revelar dados pessoais sensíveis.

§2º O tratamento de dados pessoais sensíveis não poderá ser realizado em detrimento do titular, ressalvado o disposto em legislação específica.

§3º **A menos que o titular tenha consentido adequadamente, o** disposto ~~**na alínea "c" do inciso II**~~ **no inciso IV do art. 7º** não se aplica caso as atividades de pesquisa estejam vinculadas a qualquer das seguintes atividades:

I - comercial;

II - de administração pública, quando a pesquisa não for a atividade principal ou legalmente estabelecida do órgão; ou

III - relativa à investigação criminal ou inteligência.

§4º Nas hipóteses do parágrafo anterior, sempre que possível, será garantida a anonimização dos dados pessoais.

§5º Nos casos de aplicação do disposto ~~**nas alíneas "a" e "b" do inciso II**~~ **nos incisos II e III do art. 7º** pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do art. 24.

3. A lei deve estimular meios suficientes e eficientes para promover o seu cumprimento (*accountability*):

Mais do que buscar uma definição ampla e proibitiva de dados pessoais, ou prever sanções draconianas e pouco inovadoras — como as que podem equivaler ao bloqueio de serviços legítimos ou à responsabilização objetiva (sem culpa) —, o incentivo legal a programas de cumprimento da lei (*accountability*) tem demonstrado um efeito prático muito mais significativo no sentido de estimular a adoção duradoura e sustentável de melhores práticas para a proteção dos dados pessoais. Incentivos dessa natureza já são uma realidade em países como o México, a Colômbia e a Austrália, por exemplo, e o PL 5276 andou bem nesse sentido ao estimular os programas corporativos de boas práticas previstos em seu art. 50, conforme passamos a comentar em maior detalhe.

3.1. [art. 50] A lei deve promover a implementação de programas de boas práticas em privacidade

A implementação de programas de boas práticas em privacidade, individualmente ou no âmbito de grupos de empresas, prevista no art. 50 do PL 5276 é um grande avanço do projeto. Este dispositivo previu o desenvolvimento de programas que incluem condições de organização, regime de funcionamento, procedimentos, normas de segurança, padrões técnicos e obrigações específicas para os diversos envolvidos no tratamento de dados, além de ações educativas e mecanismos internos relacionados ao tratamento de dados pessoais.

Esse avanço pode ser mais efetivo caso o art. 50, já num primeiro momento e dadas as especificações traçadas nos incisos VII e IX no art. 5º, esclarecesse que se aplica igualmente aos responsáveis e operadores nas operações de tratamento de dados — não só porque ambos podem se beneficiar dos programas de boas práticas, mas também porque podem maximizar os benefícios e a proteção para os titulares de dados mediante a sua implementação.

Para aprimorar a avaliação de risco prevista para esses programas, o §1º do art. 50 poderia considerar, além da probabilidade e da gravidade dos riscos de danos aos indivíduos, os potenciais benefícios do tratamento dos dados para seus titulares. Embora o tratamento de dados, como qualquer atividade, possa acarretar riscos, em muitos casos podem ser tomadas medidas adequadas para mitigá-los, e assim ampliar os benefícios decorrentes do tratamento. Assim, deve-se incentivar a incorporação da noção de "mitigação de riscos" como uma boa prática que faz parte da avaliação de risco.

Como um aprimoramento final, o PL 5276 também poderia incorporar incentivos específicos para que se implementem programas de boas práticas efetivos, seja para mitigar as penas previstas em lei ou para criar mecanismos de

presunção de cumprimento da lei — facilitando, por exemplo, os casos de transferências internacional de dados, ou diminuindo a frequência de auditorias de rotina ou o escopo de eventuais investigações. Essas já são práticas reconhecidas por autoridades de fiscalização e proteção de dados de diferentes países, como o México e a Colômbia, e podem ser especificamente previstas ou tornadas mais claras na lei.

Com base nessas considerações, sugerimos as seguintes emendas aos arts. 50 e 52, §1º:

> **Art. 50.** Os **operadores e** responsáveis pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão **e mitigação de riscos** e outros aspectos relacionados ao tratamento de dados pessoais.
>
> §1º Ao estabelecer regras de boas práticas, o responsável pelo tratamento e o operador levarão em consideração a natureza, o escopo e a finalidade do tratamento dos dados e a probabilidade e a gravidade dos riscos de danos, **assim como os benefícios** aos indivíduos **decorrentes do tratamento de seus dados**.
>
> §2º As regras de boas práticas serão disponibilizadas publicamente e atualizadas e poderão ser reconhecidas e divulgadas pelo órgão competente.
>
> **§3º A adoção de regras de boas práticas efetivas gera, junto ao órgão competente, a presunção em favor do cumprimento desta Lei por parte dos respectivos responsáveis e operadores.**
>
> **Art. 52.** As infrações realizadas por pessoas jurídicas de direito privado às normas previstas nesta Lei ficam sujeitas às seguintes sanções administrativas aplicáveis pelo órgão competente:
>
> [...]
>
> §1º As sanções serão aplicadas fundamentadamente, isolada ou cumulativamente, de acordo com as peculiaridades do caso concreto e com a

gravidade e a natureza das infrações, a natureza dos direitos pessoais afetados, a existência de reincidências, a situação econômica do infrator**, a adoção de regras de boas práticas, nos termos do art. 50 desta Lei,** e os prejuízos causados.

3.2. [art. 52, IV-VII] A lei deve evitar sanções equivalentes ao bloqueio do funcionamento de empresas baseadas no tratamento de dados no país

As sanções previstas entre os incisos IV e VII do art. 52 (bloqueio dos dados pessoais, suspensão de operação de tratamento de dados pessoais, cancelamento dos dados pessoais e suspensão do funcionamento de banco de dados), na prática, podem equivaler ao bloqueio no país das atividades de empresas baseadas majoritariamente no tratamento de dados. Dentre os afetados por tais medidas desproporcionais estão não apenas plataformas que possibilitam a aproximação entre empresas e clientes efetivos e potenciais ou a comunicação entre as pessoas, como também bancos de dados públicos e privados, plataformas de compartilhamento de informações urbanas e de dados de transporte, plataformas de transporte ou de hospedagem compartilhada, empresas financeiras ou de crédito, empresas baseadas na agricultura de precisão, empresas de tecnologia médica, enfim, um amplo espectro da indústria — sendo que os maiores prejudicados muitas vezes são os próprios cidadãos.

Apenas para citar o exemplo da Internet, como um relatório recente da ONG Access Now demonstra, nos últimos anos os atos de bloqueio parcial ou total da Internet têm ocorrido em diversos países, como a Índia, o Iraque e Uganda. Esses atos de bloqueio violam diretamente o direito fundamental das pessoas de receber e transmitir informações, impedindo que elas se comuniquem com seus familiares e amigos em situações corriqueiras ou de emergência, além de causar um indesejável impacto negativo na economia dos países afetados pelos bloqueios. Segundo dados da pesquisa divulgada pela ONG Access Now, os bloqueios totais ou parciais da Internet têm uma relação estreita com as leis dos países, tendo maiores chance de acontecer em países com leis retrógradas, muito amplas ou pouco transparentes.

De modo a evitar os excessos que dispositivos tendentes a permitir o bloqueio de atividades econômicas legítimas no país podem ensejar, sugerimos que sejam excluídos os incisos IV, V, VI e VII do art. 52 do PL 5276:

> **Art. 52.** As infrações realizadas por pessoas jurídicas de direito privado às normas previstas nesta Lei ficam sujeitas às seguintes sanções administrativas aplicáveis pelo órgão competente:
>
> I - multa simples ou diária;
>
> II - publicização da infração;
>
> III - anonimização dos dados pessoais;

~~IV - bloqueio dos dados pessoais;~~

~~V - suspensão de operação de tratamento de dados pessoais;~~

~~VI - cancelamento dos dados pessoais;~~

~~VII - suspensão de funcionamento de banco de dados.~~

3.3. [art. 34, §1º] A regra da responsabilidade objetiva na hipótese de transferência internacional de dados é desnecessária

A regra de responsabilidade objetiva estabelecida na parte final do §1º do art. 34 contraria não apenas a regra geral sobre a responsabilidade civil estabelecida no Código Civil Brasileiro (art. 927, *caput*, "Aquele que, por ato ilícito, causar dano a outrem, fica obrigado a repará-lo"), segundo a qual só quem efetivamente causa dano deve ser considerado responsável e obrigado ao ressarcimento, como também a regra geral de responsabilidade e ressarcimento de danos aplicável ao tratamento de dados pessoais erigida no art. 42 do próprio PL ("Todo aquele que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, é obrigado a repará-lo"), que é (e deveria mesmo ser) uma regra de responsabilidade subjetiva.

Entendemos que a regra de responsabilidade subjetiva já é suficiente para cobrir as hipóteses de transferência internacional de dados, sujeitando de forma direta o responsável pelo tratamento a reparar qualquer dano que venha a causar a outrem, em razão do exercício das atividades de tratamento, quer se trate de dano patrimonial, moral, individual ou coletivo. Mesmo que assim não se entenda, deve-se ter em mente que os casos de transferência (internacional ou não) de dados já encontra um regime de responsabilidade intensificado pela previsão da responsabilidade solidária entre cedente e cessionário, conforme o art. 44 do próprio projeto de lei, e da inversão do ônus da prova, conforme o Parágrafo Único do art. 42 do projeto — o que mais ainda reforça o argumento pela dispensa do encargo da responsabilidade objetiva nas transferências internacionais de dados.

Mesmo que assim não se entenda e a regra da responsabilidade objetiva prevaleça para as transferências internacionais de dados como regra geral, seria importante que o PL 5276 incorporasse incentivos específicos para a implementação de programas de boas práticas efetivos, sejam eles implementados conforme disposto no art. 50 ou mediante selos, certificados e códigos de conduta organizacionais emitidos por terceiros qualificados e aprovados pela autoridade competente, confirme o art. 34. Esses mecanismos serviriam não apenas para facilitar as transferências internacionais de dados, como também para criar um ambiente institucional de maior confiança e responsabilidade para que essas transferências ocorram. Reconhecendo esse

benefício, a lei deveria prever hipóteses de exclusão ou, ao menos, atenuação da responsabilidade objetivamente auferida nas transferências internacionais quando as partes envolvidas adotem aqueles programas de boas práticas ou sejam assinaladas por aqueles selos, certificados e códigos de conduta organizacionais emitidos por instituições qualificadas e/ou internacionalmente reconhecidas. Essas já são práticas reconhecidas por autoridades de fiscalização e proteção de dados de diferentes países, como o México e a Colômbia, e, enquanto mecanismos atenuantes ou excludentes da responsabilidade, podem ser especificamente previstas ou tornadas mais claras na lei. Vale lembrar que mesmo diplomas do direito brasileiro que reconhecem a regra da responsabilidade objetiva, como o Código de Defesa do Consumidor, preveem expressamente hipóteses excludentes de responsabilidade, como os casos de culpa exclusiva da vítima ou fato de terceiro (CDC, art. 12, §3º, III e art. 14, §3º, II).

Assim sendo, sugerimos que a parte final do §1º do art. 34 seja removida:

> § 1º O órgão competente poderá elaborar cláusulas contratuais padrão ou homologar dispositivos constantes em documentos que fundamentem a transferência internacional de dados, que deverão observar os princípios gerais de proteção de dados e os direitos do titular, garantida a responsabilidade solidária do cedente e do cessionário~~**, independentemente de culpa**~~.

4. [Art. 9º] A regra do consentimento livre, informado e <u>inequívoco</u> deve prevalecer sobre regras de consentimento <u>expresso</u>

A regra geral do consentimento livre, informado e <u>inequívoco</u> trazida pelo PL 5276 é um importante e necessário avanço, garantindo a um só tempo a plena manifestação do consentimento e a não exigência de modos rígidos para a sua manifestação, o que seria incompatível com o dinamismo dos negócios baseados no uso da Internet.

Entende-se que o consentimento <u>expresso</u> deve ser prestado por meios formais, com cláusulas destacadas e manifestação por escrito do titular dos dados. Já o consentimento <u>inequívoco</u>, acertadamente erigido pelo projeto como regra geral para a manifestação do consentimento para o tratamento de dados pessoais, é entendido como uma declaração ou comportamento afirmativo, ou ainda como uma ausência de comportamento negativo do titular, e pode ser prestado de forma eficaz e completamente hábil a proteger os direitos e interesses dos titulares de dados ao tempo em que também se compatibiliza com o dinamismo do uso da Internet. O consentimento inequívoco pode ser prestado não apenas por meio de declarações em cláusula destacada e por escrito pelo titular, como também por meios eletrônicos e declarações orais, incluindo marcar uma alternativa ("ticking a box")

ao visitar um website, optar por determinadas configurações técnicas para o processamento de dados e informações pessoais, ou qualquer outra forma de declaração ou conduta que inequivocamente indique a aceitação ou ausência de oposição do titular quanto ao tratamento dos seus dados pessoais. O consentimento inequívoco — diferentemente do expresso — ajuda a evitar práticas altamente indesejáveis e prejudiciais à experiência dos usuários da Internet, como a chamada "fadiga do consentimento" causada pelo excesso de requisições formais de prestação de consentimento expresso, que acaba resultando na prestação mal informada do consentimento, em grave prejuízo aos titulares.

Além disso, uma lei sobre proteção de dados seria amplamente aplicável no país, atingindo o tratamento de dados pessoais feito seja por pessoa natural, seja por pessoa jurídica de direito público ou privado (art. 1º), sejam os dados coletados por meios físicos, digitais ou por meio do uso da Internet. Mas o Marco Civil da Internet poderia vir a ser interpretado como lei específica no que diz respeito ao tratamento de dados mediante o uso da Internet no Brasil e, com base nisso, alguns poderiam argumentar pela prevalência da regra do consentimento expresso do art. 7º, VII e IX do Marco Civil, dada a sua especificidade no caso do tratamento de dados realizados mediante o uso da Internet.

Essa interpretação poderia levar a uma situação absurda em que o consentimento necessário para o tratamento de dados feito mediante o meio mais dinâmico e propenso à inovação, como é a Internet, seria mais rígido (livre, informado e expresso, devendo necessariamente ocorrer de forma destacada das demais cláusulas contratuais, conforme o art. 7º, VII e IX do Marco Civil da Internet) do que o exigível para o tratamento de dados por outros meios (livre, informado e inequívoco, podendo ser fornecido não só por escrito como por qualquer outro meio que o certifique, com base no art. 9º do PL 5275/2016).

Para evitar esse risco, sugerimos que o *caput* do art. 9º do PL 5276 seja emendado para dispor de modo expresso que a regra do consentimento livre, informado e inequívoco se aplica inclusive ao tratamento de dados feito mediante o uso da Internet, com expressa revogação dos dispositivos em contrário dispostos no Marco Civil da Internet e em seu decreto regulamentador. Para tanto e em nome da segurança jurídica, sugerimos também abaixo a inclusão do art. 57 ao projeto, com expressa menção à revogação dos dispositivos em contrário no Marco Civil e no Decreto 8.771/2016:

> **Art. 9º.** O consentimento previsto no art. 7º, inciso I, **inclusive quando o tratamento se der mediante o uso da Internet,** deverá ser livre, informado e inequívoco e fornecido por escrito ou por qualquer outro meio que o certifique.
>
> **Art. 57. Esta lei revoga as disposições em contrário, especificamente os incisos VII, VIII, IX e X do artigo 7º da Lei**

Federal nº 12.965/2014 e os artigos 13 e 14 do Decreto nº 8.771/2016.

5. [art. 3º] O escopo territorial de aplicação da lei deve ser dimensionado de modo a evitar conflitos de lei e o desestímulo às atividades de empresas multinacionais no país

Conforme seu texto atual, o projeto de lei potencialmente se aplicaria a responsáveis (nos termos do art. 5º, VIII) com sede fora do Brasil. O mais aconselhável é bem delimitar esse escopo territorial de modo que a lei só seja aplicável a responsáveis com sede no Brasil e quando o tratamento dos dados vise especificamente aos dados de pessoas com residência no Brasil. Assim, deve estar mais claro na lei que, por exemplo, ela não deve se aplicar ao processamento de dados de estrangeiros (pessoas sem residência no Brasil) por operadores (nos termos no art. 5º, IX) com sede no Brasil em nome de responsáveis estrangeiros, do mesmo modo que não se aplicaria ao processamento de dados de brasileiros que utilizem portais online sem domínio brasileiro (por exemplo, com domínio .com, e não .br). Dessa forma, responsáveis e operadores podem ter mais certeza e segurança jurídica sobre as suas obrigações e consequentemente também os titulares dos dados terão mais certeza a respeito da lei que protege os seus dados.

Impor a lei brasileira de proteção de dados a responsáveis estrangeiros criaria impedimentos significativos para a indústria brasileira de serviços de TI, bem como para outros operadores com sede no Brasil que prestem serviços a clientes globais. Operadores com sede no Brasil que processam dados em nome de seus clientes estrangeiros devem ser capazes de atender aos requisitos da legislação estrangeira relevante, isto é, da legislação aplicável aos dados no local em que são coletados. Por exemplo, se um operador brasileiro processa dados em nome de um controlador belga, o operador brasileiro deve ser capaz de aplicar a lei belga relevante a esses dados — sem a barreira de enfrentar seus pontos de conflito com a lei brasileira. Isso não significa que esse processador com sede no Brasil estaria completamente livre da aplicação plena da lei (já que a lei belga seria plenamente aplicável à sua operação) ou que o Brasil se tornaria um local de *forum shopping* para operadores maliciosos. Mesmo nesses casos, esses mesmos operadores poderiam se submeter, no mínimo, às regras brasileiras sobre programas de boas práticas (art. 50), se assim previsto na lei brasileira como um requisito mínimo para mitigar pontos de conflito com leis de proteção de dados estrangeiras e, ainda assim, garantir um grau de adequação suficiente e razoável com o direito brasileiro.

Além disso, uma consequência provável de uma regra de jurisdição tal como atualmente previsto no art. 3º do projeto é gerar conflitos com as leis de privacidade de outros países já aplicáveis às atividades de empresas sediadas em seus territórios mas que atuam globalmente e pretendem também atuar no Brasil, gerando assim

um desincentivo para que empresas estrangeiras venham a abrir escritórios no Brasil. Com isso, o Brasil passa a contar com ainda menos incentivos para atrair as atividades de empresas globais, afastando a possibilidade de protagonismo do país no mapa da inovação mundial. Regras mais flexíveis sobre proteção de dados, ao lado de outros aspectos jurídicos e extrajurídicos, têm sido apontadas por especialistas no tema, como o professor da Universidade da Califórnia, Anupam Chander, como uma das grandes responsáveis pela existência de grandes centros de inovação como o Vale do Silício (*cf.* "How law made the Silicon Valley", 2014).

Outro risco é que, com base no princípio da reciprocidade, consagrado pelo Direito Internacional Público para reger as relações entre os Estados, outros países se aproveitem do amplo escopo de aplicação da lei de proteção de dados brasileira para também tentar aplicar suas leis de proteção de dados a atividades de empresas brasileiras ou ao processamento de dados vinculados ao Brasil, ainda que as as respectivas empresas não tenham sede em tal país estrangeiro. Isso reforçaria ainda mais o risco de conflito de leis, trazendo mais instabilidade e insegurança jurídica para a operação de empresas multinacionais.

Para evitar o risco de conflito de leis e a consequente insegurança jurídica e desestímulo aos negócios que tais conflitos têm o potencial de gerar, sugerimos que seja dada ao art. 3º a seguinte redação:

> **Art. 3º. Esta Lei aplica-se ao responsável pelo tratamento de dados pessoais, quer se trate de pessoa física ou jurídica, de direito público ou privado, cuja sede esteja localizada no Brasil.**
>
> **§ 1o. Esta lei também se aplica ao tratamento de dados realizado no exterior quando a coleta, armazenamento ou utilização dos dados pessoais ocorrer em local onde seja aplicável a lei brasileira por força de tratado ou convenção.**
>
> **§ 2o. Se a lei do país onde está sediado o responsável pelo tratamento de dados pessoais garantir proteção igual ou superior à lei brasileira, aplicar-se-á ao respectivo operador sediado no Brasil a lei estrangeira no que couber.**

6. [arts. 33 e 34] A lei deve prever diversas bases legais paras as transferências internacionais de dados

A previsão de bases legais amplas para as transferências internacionais de dados, com o reconhecimento de uma série de mecanismos legítimos para além da regra da adequação, como o consentimento, o cumprimento de compromissos

assumidos em acordo de cooperação internacional e a tutela da vida e da incolumidade física dos titulares, dentre outros, são marcas da maturidade e da neutralidade tecnológica do PL 5276. É especialmente bem-vinda a incorporação de mecanismos amplamente aceitos como as "cláusulas contratuais padrão", "padrões corporativos globais" e "regras corporativas globais" (conhecidos na Europa como "Binding Corporate Rules" ou "BCRs"), posicionando o Brasil no cenário das transferências internacionais de dados.

Contudo, mesmo as cláusulas contratuais padrão e as normas corporativas globais têm as suas limitações: as primeiras não são flexíveis e podem resultar em complexidades indesejáveis, e as últimas limitam-se a transferências dentro de um grupo corporativo. Assim, para que o Capítulo sobre a Transferência Internacional de Dados do PL 5276 seja ainda mais aprimorada e ecoe ainda mais a natureza global dos fluxos de dados modernos e das atividades econômicas a ele atreladas, o art. 33 deve incluir a previsão de mecanismos como selos, certificados e códigos de conduta organizacionais emitidos por terceiros qualificados e aprovados pela autoridade competente — são opções já disponíveis em outras jurisdições, com o benefício de não se limitarem às transferências dentro de um mesmo grupo corporativo.

Um exemplo marcante da adoção desses mecanismos é o sistema do *Cross-Border Privacy Rule* (CBPR), desenvolvido e adotado no âmbito do Foro de Cooperação Econômica Ásia-Pacífico (APEC), e as certificações da União Europeia, no âmbito do GDPR, ambos com o objetivo de assegurar mecanismos de transferência de dados que permitam transferências não apenas dentro de um mesmo grupo corporativo global, mas também entre empresas não afiliadas. O México também está dando passos nesse mesmo sentido e recentemente colocou em prática um mecanismo de auto-regulação com o objetivo de se compatibilizar com o sistema CBPR e permitir fluxos de dados ainda mais seguros e confiáveis (http://www.dof.gob.mx/nota_detalle.php?codigo=5346597&fecha=29/05/2014). Selos, certificados e códigos de conduta internacionalmente reconhecidos apoiam as transferências internacionais de dados e estimulam que elas se dêem com responsabilidade e transparência.

No que diz respeito ao requisito do projeto de que apenas o "órgão competente" autorize essas regras corporativas ou códigos de conduta globais, sugerimos que seja modificado para estimular que o próprio órgão competente (1) desenvolva "cláusulas padrão" cuja adoção independa de autorização específica; (2) reconheça regras e códigos internacionalmente aceitos sem a necessidade de autorização específica; e (3) permita que organismos de certificação reconhecidos prevejam essas regras corporativas ou códigos de conduta globais, bem como aprovem e atestem a adequação das organizações a eles, de maneira semelhante ao papel desempenhado pelos chamados *Accountability Agents* no sistema APEC CBPR e de modo a evitar gargalos de aprovação no âmbito das autoridades competentes. Não é realista nem desejável impor ao órgão competente um volume desproporcional de processos

administrativos para a aprovação específica de transferências internacionais de dados — esses processos de aprovação prévia e específica devem, na verdade, ser reduzidos ao mínimo necessário e reservados aos casos excepcionais que efetivamente demandem a atenção do órgão competente. Se assim não for, o órgão competente teria que alocar praticamente a totalidade de seu tempo produtivo para analisar pedidos e processos de aprovação de transferências de dados, o que, definitivamente, não implicaria uma atuação mais estratégica do órgão, muito menos níveis de proteção significativamente maiores para os titulares dos dados.

Vale ressaltar que o Foro de Cooperação Econômica Ásia-Pacífico e a União Europeia têm explorado maneiras de racionalizar os processos de certificação e aprovação de empresas que procuram a "dupla certificação" nos dois sistemas, assim como têm explorado formas de tornar as novas certificações com relação à GDPR compatíveis e interoperáveis em relação à CBPR. Tendo em vista essa tendência, os mecanismos sobre transferência internacional de dados previstos na lei brasileira devem desde já ser projetados de modo a que também sejam interoperáveis em relação a estes e outros sistemas de cooperação similares para transferências internacionais, para garantir que as empresas que tenham recebido aprovação sob um sistema não brasileiro possam alavancar sua aprovação no Brasil e vice-versa.

Benchmark internacional sobre transferência internacional de dados:

Tomando como exemplo o cenário internacional, é válido lembrar que países como os Estados Unidos, México, Canadá e Japão não impões restrições *ex ante* à transferência internacional de dados em suas lei gerais ou esparsas sobre proteção de dados.

A lei de proteção de dados do México incorpora grande parte da orientação do quadro de privacidade de APEC, prevendo mecanismos de "accountability" e reconhecendo a necessidade e o valor da transferências internacionais de dados pessoais. A legislação mexicana também aborda de forma clara as distintas obrigações e direitos existentes na medida em que os dados pessoais são transferidas entre "controladores" e "processadores" de dados", além da documentação necessária para garantir o cumprimento das exigências legais.

Da mesma forma, o Canadá, através do PIPEDA (*Personal Information Protection and Electronic Documents Act*), adota uma abordagem "de organização para organização", que não se baseia no critério de adequação para viabilizar as transferências internacionais de dados. O PIPEDA não proíbe as organizações no Canadá de transferir dados pessoais para uma organização em outra jurisdição para fins de tratamento de dados. As organizações são responsáveis pela proteção dos dados pessoais transferidos nos termos dos acordos de transferência que lhes dão base. A autoridade de proteção de dados canadense (Office of the Privacy Commissioner) pode investigar reclamações e auditar as práticas de transferências de dados pessoais das diferentes organizações.

Em suma, dada a variedade de mecanismos disponíveis para as transferências internacionais de dados, os regimes de privacidade locais devem se concentrar em reconhecer ferramentas alternativas de co-regulação, de modo que os custos de se observar as diferentes regras internacionais aplicáveis às transferências internacionais de dados sejam razoáveis e proporcionais.

Com base nessas considerações, sugerimos as seguintes emendas ao Capítulo sobre a Transferência Internacional de Dados do PL 5276:

> **Art. 33.** A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
>
> I - para países que proporcionem nível de proteção de dados pessoais ao menos equiparável ao desta Lei;
>
> II - 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;
>
> III - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> IV - quando o órgão competente autorizar a transferência;
>
> V - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
>
> VI - quando a transferência for necessária para execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do art. 24; ou
>
> V - quando o titular tiver fornecido o seu consentimento para a transferência, com informação prévia a específica sobre o caráter internacional da operação, com alerta quanto aos riscos envolvidos.
>
> **VI - quando o responsável pelo tratamento comprovar que a transferência se baseia em cláusulas contratuais padrão aprovadas pelo órgão competente ou em regras e códigos internacionalmente aceitos;**
>
> **VII - quando o responsável pelo tratamento comprovar que detém selos, certificados ou códigos de conduta e adequação emitidos por organismos de certificação qualificados e aprovados pelo órgão competente.**
>
> Parágrafo único. O nível de proteção de dados do país estrangeiro será avaliado pelo órgão competente, que levará em conta:

I - as normas gerais e setoriais da legislação em vigor no país de destino;

II - a natureza dos dados;

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

IV - a adoção de medidas de segurança previstas em regulamento;

V - as outras circunstâncias específicas relativas à transferência.

Art. 34. A autorização referida no inciso IV do caput do art. 33 será concedida quando o responsável pelo tratamento apresentar garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular **e será dispensável nas hipóteses dos incisos VI e VII do art. 33 desta Lei.** ~~**apresentadas em cláusulas contratuais aprovadas pelo órgão competente para uma transferência específica, em cláusulas contratuais padrão ou em normas corporativas globais, nos termos do regulamento.**~~

§1º O órgão competente poderá elaborar cláusulas contratuais padrão ou homologar dispositivos constantes em documentos que fundamentem a transferência internacional de dados, que deverão observar os princípios gerais de proteção de dados e os direitos do titular, garantida a responsabilidade solidária do cedente e do cessionário~~**, independentemente de culpa**~~.

§2º Os responsáveis pelo tratamento que fizerem parte de um mesmo grupo econômico ou conglomerado multinacional poderão submeter normas corporativas globais à aprovação do órgão competente, obrigatórias para todas as empresas integrantes do grupo ou do conglomerado, a fim de obter permissão para transferências internacionais de dados dentro do grupo ou do conglomerado sem necessidade de autorizações específicas, observados os princípios gerais de proteção e os direitos do titular.

§3º Na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação do órgão competente, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento.

§4º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no caput serão, também, analisadas de acordo com o previsto nos §1º e §2º do art. 45.