Centre for Information Policy Leadership
Hunton & Williams LLP

5 abril de 2017 (1 Junho de 2017)

PONTOS DE DISCUSSÃO

PROJETO DE LEI NO 5276/2016, DO PODER EXECUTIVO,

DE PROTEÇÃO DE DADOS

1. Comentários Gerais

A CIPL considera bem-vindo o reconhecimento feito no Artigo 2 de que a lei de proteção de dados não está fundamentada somente na necessidade de proteger a privacidade dos indivíduos, mas também precisa ser consistente com a liberdade de expressão, o desenvolvimento econômico e tecnológico, a livre inciativa e a livre concorrência.

A CIPL também acredita que o projeto de lei atual inclui vários aprimoramentos significativos com relação a versões anteriores do projeto. Por exemplo, consideramos muito bem-vinda a inclusão do fundamento dos "interesses legítimos" para o tratamento dos dados, além da inclusão da avaliação de risco e, assim, de uma abordagem com base em risco, que vemos no dispositivo sobre "boas práticas" , a previsão de um leque amplo de mecanismos que possibilitam a transferência internacional de dados e a previsão de um "órgão competente", entre outros itens.

Nos últimos anos, uma revolução digital e de dados global alterou radicalmente o cenário ao qual as leis de proteção de dados se aplicam. Vivemos hoje em uma nova "era digital" que é baseada e guiada por megadados ("*Big Data*"), pela Internet das Coisas (*Internet of Things – IoT),* Inteligência Artificial *(Artificial Intelligence – AI*) e pelo aprendizado de máquinas (*Machine Learning)*. Tudo são dados e dados estão por toda a parte. Dados fluem no mundo em volume constantemente crescente e são utilizados em maneiras novas e cada vez mais complexas. Isso constitui uma nova realidade que tem que ser levada em consideração quando da elaboração de novas leis de privacidade e proteção de dados que se adequem a nova era de informações. O Brasil tem hoje a oportunidade singular de criar uma lei que atenda às necessidades dessa era digital, levando em consideração as experiências, erros e acertos de outros regimes de privacidade pelo mundo. A maioria, quiçá todos, desses regimes de privacidade que existem historicamente foram projetados antes da era digital e também enfrentam hoje a necessidade de se modernizarem

Nesse sentido, é importante evitar criar leis que se tornem obsoletas na medida em que novos avanços tecnológicos ocorrem ou cujo impacto não seja compreendido de todo por

ocasião de sua elaboração e redação e que, portanto, podem acarretar consequências não intencionais para usos legítimos de dados e seu aproveitamento. Naturalmente, as organizações que irão cumprir com essas disposições estarão em melhor posição para prever essa consequências em potencial. Assim, recomendamos fortemente que, como parte de consultas envolvendo múltiplos *stakeholders*, essas organizações sejam consultadas extensivamente com relação a detalhes de quaisquer disposições finais.

Objetivando atender as demandas dessa nova era digital e estar blindado para o futuro, acreditamos que a lei de proteção de dados no Brasil deverá conter as seguintes características-chave:

1. **Ser claras e fáceis de entender, aplicar e fazer valer.** Essa lei tem um escopo abrangente de aplicação e seria aplicável a todos os dados pessoais (de cidadãos, clientes, empregados, contatos de negócios) e cobriria todos os setores industriais e empresas comerciais de todos os portes, inclusive setores que não têm experiência no tema da proteção de dados e pequenos negócios que não têm experiência ou capacidade para contratar uma diretoria de proteção de dados para ajudar na observância da lei. É essencial que os requisitos sejam simples, fáceis de compreender e de implementar de forma geral.

2. **Seguir uma abordagem baseada em princípios.** Em vez de requisitos demasiadamente específicos e detalhados, devem ser considerados princípios maiores e "objetivos" que permitam às organizações aplicá-los de forma flexível, com base em análises de benefícios/riscos apropriadas que por sua vez determinarão as medidas de proteção de dados específicas apropriadas para um determinado contexto, particularmente conforme a tecnologia, as práticas de negócios e as expectativas das pessoas evoluem.

3. **Incluir uma abordagem baseada em risco.** Isso significa que as organizações deverão entender os riscos e danos aos titulares causados por qualquer tratamento de dados, bem como os benefícios do tratamento, e ser capazes de calibrar a observância da lei com os riscos e danos em potencial. Dessa maneira, poderão concentrar em seus esforços de observância, ações de mitigação e responsabilização nas áreas que podem causar riscos e danos. Igualmente, não deveriam depreender muitos esforços nas áreas que não criam riscos e danos a indivíduos, tais como no contexto do tratamento de dados B2B, ou outros usos comuns e ordinários dos dados.

4. **Permanecer tecnologicamente neutra.** (ex. em questões sobre segurança de dados) para que a lei possa se adaptar a mudanças tecnológicas e permanecer relevante.

5. **Estabelecer uma variedade de bases legais para o tratamento e as transferências de dados.** A lei deve incluir uma gama ampla de fundamentos para o tratamento de dados, do consentimento aos interesse legítimos, cada qual podendo ser aplicado pragmaticamente em contextos apropriados para permitir usos benéficos dos dados na era da informação, ao mesmo tempo em que protege também o titular. A lei também deve prever um leque amplo de mecanismos para a transferência internacional de dados, que espelhem e sejam capazes de operar com todos os outros mecanismos de transferência internacional, permitindo que os dados fluam de forma contínua por todo o globo – o que é essencial tanto para a economia moderna quanto para o uso de dados para fins comerciais e para o progresso social.

Em nossa opinião, o projeto atual cobre boa parte dessas recomendações. Todavia, os comentários mais detalhados abaixo sobre disposições-chave do projeto poderiam ajudar a aprimorar a lei com base nesses conceitos.

2. Finalidade da lei de proteção de dados (Artigo 2)

Mensagem principal: É útil e apropriado que a lei de proteção de dados reflita interesses e valores adicionais, e às vezes concorrentes, que devem ser levados em consideração e ponderados quando protegendo a privacidade pessoal, tais como permitir inovação, desenvolvimento econômico e avanços sociais.

- Consideramos muito bem-vindo o reconhecimento de que as leis de proteção de dados devam não somente proteger a privacidade, mas também outros valores, incluindo a inovação e o uso responsável dos dados para o desenvolvimento econômico, social e tecnológico.
- Igualmente, as autoridades de proteção de dados têm hoje um **papel duplo**: de proteção da privacidade de um lado e, do outro, de possibilitar o uso responsável dos dados na moderna economia e sociedade baseadas em dados.

3. Necessidade de distinguir entre o responsável e o operador; âmbito de aplicação da lei (Artigo 3)

Diferença entre responsável e operador

Centre for Information Policy Leadership
Hunton & Williams LLP

5 abril de 2017 (1 Junho de 2017)

Mensagem principal: Incentivamos que a lei esclareça a diferença entre responsável e operador, definindo seus papéis e responsabilidades distintas na proteção dos dados.

- Em geral, o projeto de lei aparentemente reconhece que os responsáveis pelo tratamento dos dados são as organizações que coletam e usam os dados pessoais para fins diversos, tomam todas as decisões com relação ao tratamento dos dados e podem apontar operadores de dados terceiros para realizar funções variadas.
- Embora o texto não faça referência explícita aos operadores, ele corretamente permite que se entenda que o operador atua somente por conta do responsável e executa requisitos legais meramente consoante as instruções que receba do responsável e seu vínculo contratual.
- Preocupa, todavia, que essa distinção não esteja prevista explicitamente ou refletida de forma consistente no texto do projeto. A CIPL acredita que o projeto de lei se beneficiaria da inclusão dessa distinção em seu Capítulo I, Artigo 3, onde o escopo de aplicação da lei é definido, e em seu Artigo 6, que define os princípios para o tratamento de dados. Do modo como o projeto está escrito hoje, essas disposições aparentemente aplicam-se igualmente tanto aos responsáveis como aos operadores no Brasil.
- Incentivamos que o texto do projeto apresente uma melhor distinção entre responsáveis e operadores, e suas respectivas atribuições.

Escopo de aplicação da lei

Mensagem Principal: A regra sobre o âmbito de aplicação da lei deveria deixar claro que a lei de proteção de dados brasileira não se aplica ao tratamento de dados estrangeiros por operadores brasileiros atuando em nome de responsáveis estrangeiros/não brasileiros. Em geral, a lei deveria aplicar-se às organizações (responsáveis ou operadores) estabelecidas no Brasil, independentemente de onde processam os dados. Outrossim, o tratamento de dados pessoais de brasileiros que realizam compras online em domínios/websites não-brasileiros (ex. em site .com ao invés de .br) não deveria estar subordinado a essa lei.

- Em geral, é positivo que o escopo regra sobre o âmbito de aplicação da lei tenha sido devidamente restringido para refletir mais de perto as disposições usuais de jurisdição previstas em leis de proteção de dados de outros países globalmente.

- Todavia, acreditamos que o escopo da lei continua demasiadamente amplo, eis que o Art. 3(1) potencialmente abarcaria responsáveis estrangeiros e operadores brasileiros atuando por conta de responsáveis estrangeiros. Nesses casos, os dados dos titulares poderiam estar sujeitos a requisitos de tratamento estrangeiros que gerem conflito ou sobreposição com a eventual lei brasileira. O melhor seria se os titulares pudessem gozar da proteção da lei de sua jurisdição e os operadores ficassem responsáveis pelo tratamento de dados na forma dessas mesmas regras.
- Impor a lei de proteção de dados brasileira a responsáveis estrangeiros criaria impedimentos significativos para a indústria brasileira de serviços TI Acreditamos que a lei deveria declarar explicitamente, em referências ao dispositivo sobre Boas Práticas, que ela também se aplica a operadores e operações de tratamento dentro do território nacional. (Discutimos esta questão em mais detalhes abaixo no tópico sobre Boas Práticas).
- Finalmente, também acreditamos que responsáveis estrangeiros não deveriam em geral estar subordinados à lei brasileira de proteção de dados quando os consumidores brasileiros adquirem produtos em domínios/websites não brasileiros tais como. com (ao invés de .br).

4. Consentimento – Dados Sensíveis (Artigo 11)

Mensagem Principal: Deve-se tomar cuidado que as disposições sobre consentimento relacionadas a dados sensíveis não se tornem tão restritivas a ponto de impedir o uso benéfico desses dados – com salvaguardas apropriadas.

- A CIPL está preocupada que as disposições de consentimento relacionadas a dados sensíveis sejam restritivas demais e não reflitam a realidade sobre o uso desses dados nos dias atuais.
- Exigir consentimento expresso para o tratamento de dados sensíveis impedirá um grande número de possibilidade de usos benéficos desses dados (inclusive usos que não tenham valor comercial mas que beneficiariam a sociedade), onde o responsável não está em posição de obter o consentimento expresso ou em situações em que o consentimento é recusado sem justificativa mesmo quando o tratamento não implica em qualquer dano, por exemplo. Assim, somos a favor de permitir que interesses legítimos sirvam de base para o tratamento de dados sensíveis. Em razão de o interesse legítimo demandar uma avaliação de risco

bem como das mitigações apropriadas, ele atuará como barreira protetora dos dados pessoais bem mais do que o consentimento expresso poderia.

- Também sugerimos que a liberação de pesquisa seja esclarecida para incluir explicitamente a pesquisa que é "associada" a atividades comerciais. Hoje em dia, uma grande parte da pesquisa que beneficia a sociedade é conduzida por empresas. As organizações deveriam poder usar dados sensíveis, seja para fins comerciais ou objetivos mais amplos que beneficiem a sociedade, desde que os dados sejam tratados com responsabilidade e que o risco de dano seja nulo ou muito baixo.
- Sobre este ponto, gostaríamos por fim de chamar atenção para a proposta legislativa contida no Projeto de Lei 6291/2016, que tramita em conjunto com o PL 5276. Este projeto busca modificar o Marco Civil da Internet, trazendo uma definição demasiadamente ampla de dados pessoais (que se mistura com exemplos de dados sensíveis), além de prever uma regra geral de não compartilhamento de dados, exceto quando o compartilhamento se dê mediante "consentimento livre, inequívoco, informado expresso e específico". A CIPL acredita que esta proposta legislativa não reflete a realidade atual sobre o tratamento de dados e tem o potencial de inibir a possibilidade de usos e compartilhamentos benéficos de dados pessoais e sensíveis. Acreditamos, portanto, que o PL 6291/2016 deve ser integralmente rejeitado.

5. Consentimento e interesses legítimos (Artigos 5 e 7).

Mensagem Principal: A CIPL considera muito bem-vinda a inclusão dos interesses legítimos como base legal para o tratamento de dados. Embora o consentimento permaneça sendo uma base importante para o tratamento de dados, cada vez mais nem toda forma de tratamento de dados se dá ou deveria se dar com base no consentimento. As realidades do tratamento analítico de *big data* são um exemplo crítico nesse sentido.

- **Mensagem principal com relação ao consentimento**: Quanto ao consentimento, acreditamos que quando o consentimento expresso não for obrigatório (ex., com relação a dados não sensíveis), meios válidos de consentimento deveriam incluir o *opt-out* e o consentimento implícito para assegurar que os titulares não sejam sobrecarregados com solicitações constantes de consentimento no mundo digital.
- O tratamento de dados baseado nos interesses legítimos frequentemente oferece uma base de mais "responsabilização" e é mais capaz de proteger os titulares

que o consentimento, visto que leva em conta um equilíbrio entre benefícios e riscos bem como a implementação de mitigações apropriadas.

- O Artigo 10 estabelece que o interesse legítimo deve contemplar a "legítima expectativa" dos titulares. Essa disposição restringe desnecessariamente a aplicação do interesse legítimo, que poderia ser útil nos casos em que o tratamento se refira a modos de aproveitamento dos dados de maneiras novas, desconhecidas anteriormente.
- O uso de dados accessíveis ao público não deveria estar subordinado aos requisitos de tratamento do Artigo 7.
- Sugerimos que o legislador revise as disposições sobre consentimento para deixar claro que o consentimento não é necessário quando o tratamento for para fins de desempenho de uma tarefa realizada em prol do interesse público ou no exercício de autoridade oficial investida no responsável ou em terceiro a quem os dados sejam revelados. Por exemplo, dados referentes a celulares ou sobre vizinhanças ou locais de residência poderiam ser úteis para a autoridade pública ou terceiro autorizado no caso de ajuda em situação de desastre público.

6. Princípios, Finalidade e Adequação (Artigo 6)

Mensagem Principal: Com relação à disposição sobre "finalidade", sugerimos expandir o escopo da "finalidade informadas ao titular" para incluir o que é razoavelmente esperado pelos titulares.

- "Informado" parece impor um dever específico ao responsável pelo tratamento de dados, sendo que em muitos casos o indivíduo pode razoavelmente esperar que os dados sejam usados de determinadas maneiras como uma prática normal no curso das atividades ou padrões sociais.
- Com relação à disposição sobre "adequação", acreditamos que seria melhor fornecer uma orientação adicional sobre como a "adequação" deve ser determinada. Seria útil incluir uma disposição estabelecendo que os responsáveis deverão levar em consideração:
    - Qualquer vínculo entre as finalidades originais pretendidas e os objetivos do tratamento continuado;
    - O contexto em que os dados foram coletados e tratados
    - A natureza dos dados pessoais;
    - Qualquer impacto do tratamento continuado sobre os titulares, incluindo as chances e a gravidade de eventuais prejuízos para os titulares; e

- A existência de salvaguardas apropriadas.

Se a finalidade do tratamento continuado não for "adequada", qualquer tratamento futuro deverá se dar em conformidade com as disposições do Artigo 7, incluindo o consentimento ou interesses legítimos.

7. Danos Anônimos (Artigos 5 e 13)

Mensagem Principal: A CIPL fica satisfeita em ver que o projeto de lei continua reconhecendo a importância dos dados anonimizados. A legislação atenderá melhor ao objetivo de proteger de dados pessoais dos brasileiros se incentivar as organizações a des-identificar ou anonimizar dados.

- Acreditamos que os dados anonimizados devem ser excluídos do âmbito de aplicação da lei quando a re-identificação seja possível tão somente através de esforços "extraordinários". Mesmo naqueles casos onde a re-identificação possa ocorrer através de esforços meramente "razoáveis", os dados ainda deveriam ser considerados anônimos e fora da abrangência da lei se a anonimização se der com base proteções legais, obrigacionais e administrativas, como por exemplo proibições contratuais e regulatórias de re-identificar dados exceto em circunstâncias específicas. Recomendamos que isso seja previsto explicitamente no Artigo 4.

8. Transferências Internacionais de Dados (Artigos 33 e 34)

Mensagem Principal: A CIPL saúda a abordagem do projeto de lei às transferências internacionais de dados na medida em que prevê um amplo leque de mecanismos que podem ser usados para legitimar transferências de dados pessoais a países que não tenham níveis similares de proteção de dados e na medida em que esses mecanismos podem trabalhar em conjunto com mecanismos similares de outros países.

- Em particular, ficamos satisfeitos com a incorporação dos conceitos largamente aceitos de "cláusulas contatuais padrão" e "normas corporativas globais" (conhecidas na Europa como *Binding Corporate Rules" ou "BCR")*. Isso posiciona o Brasil para transferências de dados com a Europa e outros países que reconhecem esses mecanismos de transferência internacional.

- Todavia, mesmo cláusulas contratuais padrão e normas corporativas globais têm suas limitações – as primeiras não são flexíveis e podem resultar em complexidade indevida, enquanto que as últimas estão limitadas a transferências dentro de um grupo societário, além de não serem escaláveis, já que dependem da aprovação do órgão competente (quando o GDPR entrar em vigor, as BCRs provavelmente também poderão ser utilizadas entre diferentes grupos societários).
- Assim, embora incentivando o Brasil a incluir essas opções, também encorajamos o país a trabalhar com especialistas, inclusive com a CIPL, para aprimorar esses mecanismos e torná-los mais práticos e escaláveis para uso geral por empresas de todos os portes.
- Além disso, acreditamos que o menu de escolhas disponíveis para as empresas deveria ser expandido para refletir o caráter global dos fluxos de dados e das atividades econômicas nos dias de hoje e as opções já disponíveis em outros países e regiões para a transferência de dados não apenas dentro de grupos econômicos como também entre diferentes grupos. Assim, dentre as opções de mecanismos para as transferências internacionais de dados, encorajamos a inclusão de mecanismos como as Normas Transfronteiras de Privacidade da APEC (*APEC Cross-Border Privacy Rules –CBPR),* desenvolvidas pelo fórum APEC, além de certificações e selos como as Certificações da União Europeia, sob o GDPR, além dos códigos de conduta organizacionais certificados por terceiros apropriados ou por autoridades competentes.
- De fato, com relação ao requisito no projeto de lei de que o "órgão competente" autorize esses padrões ou normas societárias globais, sugerimos que seja modificado para permitir que órgãos certificadores reconhecidos autorizem esses padrões ou normas, tal como ocorre no caso *"Accountability Agents"* do sistema CBPR da APEC, de modo a evitar gargalos nas aprovações desses mecanismos pelos órgão competentes nacionais.
- Vale ressaltar que a APEC e a UE já começaram a explorar maneiras de simplificar e racionalizar a certificação CBPR/BCR e os processos de aprovação por meios dos quais as empresas buscam a "certificação dupla" sob os dois sistemas. Eles também estão explorando novas certificações da EU, sob o GDPR, compatíveis e interoperantes com relação ao sistema CBPR. Assim, a CIPL recomenda que quaisquer contrapartes brasileiras a esses mecanismos sejam projetadas de modo que também sejam interoperantes com essas e outras estruturas similares para as transferências internacionais de dados, de modo a

assegurar que as empresas certificadas, ou que receberam aprovação sob uma estrutura não-brasileira, possam alavancar a respectiva aprovação no Brasil e vice-versa.

9. Comunicação de Incidentes de segurança (Artigos 47 e 48)

Mensagem Principal: A CIPL reconhece como positiva a abordagem do projeto de quanto à comunicação de eventual incidente de segurança à autoridade competente e/ou aos indivíduos, demandando que essa comunicação seja feita em "prazo razoável" após fatos sobre o incidente serem apurados e quando a violação possa acarretar risco substancial ou prejuízo relevante para o titular.

- O projeto de lei permite que ao *órgão competente* defina um "prazo razoável" dentro do qual o responsável deverá informar a autoridade sobre a ocorrência de incidente que acarrete risco ou prejuízo relevante para os titulares. A CIPL fica considera essa abordagem muito bem-vinda, ressalvando que a lista de itens a ser incluída na comunicação demonstra o reconhecimento pelo legislador de que as empresas precisam de tempo para estabelecer os fatos e a natureza da violação, para determinar quais dados que foram impactados, qual foi o impacto, e quais foram os riscos e danos resultantes da violação, bem como as medidas de mitigação que tenham sido ou venham a ser tomadas. Leva tempo para empreender essa análise pericial forense e jurídica e não faz sentido comunicar e onerar pessoas e autoridades até que os fatos sejam conhecidos e os riscos e prejuízos em potencial sejam avaliados. Além disso, em algumas circunstâncias, é importante não revelar aos titulares ou ao público que uma violação ocorreu enquanto estiver pendente uma investigação criminal não pública ou outro tipo de investigação.
- Com relação à notificação aos titulares, o projeto de lei prevê que eles receberão "pronta comunicação" independentemente de determinação do órgão competente, "nos casos em que for possível identificar que o incidente coloque em risco a segurança pessoal dos titulares ou lhes possa causar danos". Isso também implica um tempo razoável durante o qual a organização poderá estabelecer essa possibilidade, isto é, a natureza e possível risco ou dano, dentre outras questões.
- A encriptação não é prevista com uma exceção a estas exigências no projeto de lei. Assim, mesmo quando os dados ou o aparelho estejam encriptados, o

incidente de segurança deverá ser comunicado. Acreditamos, porém, que o nível para acionamento do requisito de comunicação de incidentes de segurança com relação a dados encriptados deveria ser mais elevado. Se a avaliação de risco após a violação concluir que os dados estavam suficientemente encriptados e não apresentavam risco para o titular, então a comunicação ao órgão competente ou aos titulares não deveria ser obrigatória.

- As exigências de que empresas revelem a natureza das medidas de segurança adotadas deveriam ser eliminadas ou ao menos restringidas significativamente para incluir somente a natureza geral das medidas de segurança levadas a cabo. Revelar informações demasiadas sobre segurança pode comprometer os esforços dos profissionais de remediar os eventuais incidentes, além de expor desnecessariamente os sistemas de segurança a novas situações de risco em razão de ações de criminosos.

10. Segurança (Artigo 49)

Mensagem Principal: A lei não deve estabelecer requisitos específicos de segurança; tais requisitos devem permanecer eficazes à prova do futuro, flexíveis e específicas consoante o contexto. As organizações deverão determinar as medidas apropriadas de segurança com base em padrões e práticas de última geração, nos custos, na natureza dos dados e nos riscos envolvidos.

- É contraproducente exigir que medidas de segurança sejam determinadas por leis ou regulamentos, que imediatamente fazem deles elementos ultrapassados, visto que as leis ficam defasadas com relação à tecnologia e o desenvolvimento de padrões técnicos. É mais recomendável que a determinação de medidas específicas de segurança fique a cargo das organizações e que tais medidas sejam estabelecidas com base em padrões e práticas de última geração, nos custos, na natureza dos dados e nos riscos envolvidos.
- É mais recomendável que as leis de proteção de dados incluam um requisito geral de segurança no sentido de fomentar medidas apropriadas para proteger os dados de perdas, destruição, acesso não autorizado e outras formas de tratamento ilegal (tal como consta no GDPR da União Europeia). Assim fica a cargo das organizações determinar que medidas seriam apropriadas para proteger os dados de acessos não autorizados, perda, destruição, revelações e

tratamento em qualquer contento, com base nos critérios mencionados acima.

11. Boas Práticas (Artigo 50)

Mensagem Principal: A CIPL considera muito bem-vinda esta disposição, que incorpora os conceitos de avaliação de riscos e benefícios do tratamento de dados, "accountability" organizacional (ex. programas empresarias de privacidade robustos) e códigos organizacionais ou setoriais de conduta. Devem existir incentivos claros para que as organizações, quer se tratem de responsáveis ou de operadores, adotem programas de gerenciamento de privacidade e boas práticas.

- Acreditamos que os exemplos de "boas práticas" também devem incluir procedimentos para lidar com reclamações. Para evitar sobrecarregar a autoridade competente e/ou o Judiciário, é importante (e possível) que a maioria das reclamações dos titulares sejam encaminhadas inicialmente no nível da empresa.
- Além de levar em consideração os eventuais riscos, as avaliações de risco também devem considerar os benefícios aos titulares decorrentes do tratamento de dados. Isso pode ser entendido com base na "finalidade" do tratamento, mas seria melhor fazer referências a "benefícios" explicitamente.
- Também deveria ser ressaltado que, embora o tratamento de dados possa acarretar riscos, em muitos casos medidas apropriadas podem ser tomadas para mitigá-los, permitindo assim que os benefícios do tratamento de dados sejam realizados. Assim, a lei deve incorporar uma linguagem que reflita a noção de que medidas de *mitigação de riscos* são uma boa prática e devem compor as avaliações de risco.
- Também deveriam ser estabelecidos incentivos para as empresas formularem ou adotarem esses programas de governança em privacidade, como por exemplo a autorização para lidar com um volume maior de tratamento de dados, ou a autorização para compartilhar dados, ou mecanismos para mitigar a intensidade das ações de supervisão e execução do órgão competente. Por exemplo, no caso de processo de execução, as empresas que aderissem a esses programas de governança em privacidade e fossem capazes de demostrar esforços de boa fé em seu cumprimento poderiam se sujeitar a penas mais brandas em eventual caso de violação da lei. Práticas como essas já são reconhecidas por várias

autoridades de proteção de dados de diferentes países. (Esta questão poderia ser abordada na seção sobre "Sanções Administrativas").

- Este dispositivo também deveria esclarecer que essas "normas de boas práticas" também poderiam servir como mecanismos reconhecidos para transferências internacionais de dados, conforme descrito acima na seção 8 (vide, por exemplo, o uso pela GBPR da EU de certificações e códigos de conduta como mecanismos de transferência). Assim, sugerimos que as normas de boas práticas também incluam a adoção de certificação e selos para as transferências internacionais de dados. Sugerimos ainda que as normas de boas práticas poderiam envolvam a adesão a códigos de conduta setoriais reconhecidos. Ambos promoveriam observância à lei nacional mas também serviriam como mecanismos para facilitar as transferências internacionais de dados.
- Na medida que normas, certificações e códigos de conduta forem pensados para servir como mecanismos de transferência internacional de dados, os mesmos deverão ser projetados de tal forma a lhes permitir interoperarem substancial e processualmente com estruturas similares em outros países para permitir soluções de transferência internacional para as empresas e evitar a dupla certificação de empresas já submetidas a padrões similares.
- Por fim, o texto deveria também estabelecer explicitamente que as normas de boas práticas podem aplicar-se tanto a responsáveis como a operadores, visto que ambos se beneficiariam da implementação proativa de programas de gerenciamento de privacidade e segurança.

12. Órgão Competente (Artigo 53)

Mensagem Principal: Consideramos bem-vinda a disposição que descreve o "órgão competente", sendo esse referido em vários lugares no texto do projeto de lei. Uma autoridade independente será fundamental para a implementação e cumprimento da lei com sucesso. Isso dará ao Brasil uma autoridade centralizada e especializada, tendo por missão: manter-se atualizada com relação aos desenvolvimentos da tecnologia, das práticas de mercado relevantes, das questões de privacidade e das medidas que possam tratar dessas questões de forma prática e eficaz; oferecer orientação competente e consistente e interpretar e fazer valer a lei de forma consistente; apoiar e facilitar a educação digital da população e educar as organizações e os titulares quanto aos seus respectivos direitos e obrigações; enfim representar o Brasil como "uma única voz" em qualquer questão de privacidade internacional, de desenvolvimento internacional de

políticas de privacidade e no contexto da cooperação com autoridades estrangeiras individualmente ou através das várias redes de políticas de privacidade e de aplicação de regras de privacidade globais, tais como o *Interrnational Conference of Data Protection and Privacy Commissioners (ICDPPC)* e a rede *Global Privacy Enforcement Network (GDPR)*, entre outras.

- Com relação ao inciso VI, sugerimos que a redação "que facilitem o exercício de controle dos titulares sobre seus dados pessoais" seja alterada para "que facilitem a proteção dos dados pessoais". Em resposta a tecnologias emergentes e à capacidade de tratamento de dados, medidas de proteção à privacidade têm focado cada vez menos em " controle" e cada vez mais em assegurar que os dados pessoais permaneçam seguros e protegidos, sejam tratados com responsabilidade e não sejam utilizados de forma que possa danificá-los. A redação que propomos aqui seria aplicável de forma mais abrangente e englobaria a facilitação ao exercício do controle dos titulares sobre seus dados, sempre que apropriado, recomendável e possível.
- Com relação ao inciso VIII, a publicidade e a transparência apropriadas dependem muito do contexto e não são objeto fácil de regulamentação. Ao contrário, sugerimos que este dispositivo seja deletado e substituído por redação no sentido de "fomentar e encorajar medidas eficazes de transparência e publicidade das operações de tratamento".
- Finalmente, sugerimos que um novo inciso seja adicionado a este Artigo para permitir consultas e um anal de diálogo contínuo entre a autoridade competente e as entidades reguladas e outros *stakeholders*, inclusive sobre a interpretação e a implementação apropriadas da lei, bem como sobre tecnologias emergentes.

13. Entrada em vigor (Artigo 56)

Mensagem Principal: O Brasil deve estender significativamente o prazo de 180 dias previsto neste dispositivo, de modo a oferecer às empresas tempo hábil para passarem a observar a nova lei.

- Para cumprir com lei, as companhias precisarão se familiarizar com suas disposições legais, entender como podem ser interpretadas pelos reguladores e aplicadas de forma prática, além de tomar as medidas apropriadas internamente.

Isso será particularmente trabalhoso dado que essa será a primeira lei exaustiva sobre proteção de dados no país.

- Um prazo de tempo razoável seria de no mínimo três anos. O GDPR da EU previu dois anos, mas já vislumbramos, restando apenas mais um ano para a fase de implementação se iniciar, que as organizações não estarão completamente prontas até maio de 2018.

14. Eficácia *ex nunc*

Mensagem Principal: Recomendamos fortemente que esta lei esclareça que sua aplicação se dará *ex nunc*, ou seja, a dados pessoais que forem coletados após a sua entrada em vigor, de forma voltada para o futuro e não de forma retroativa.

- A experiência demonstra que leva muito tempo para assegurar que sistemas antigos de TI e usos existentes de dados passem a observar as novas normas. Conforme as organizações enfrentam dificuldades para aplicar os novos requisitos da lei aos dados e às formas de tratamento existentes, perdem um tempo importante, que poderia estar voltado para assegurar que seus novos sistemas, formas de tratamento de dados e tecnologias estejam em conformidade com a lei.
- Assim, a lei não deveria ser aplicada retroativamente (*ex tunc*), mas sim *ex nunc*, aos dados coletados a partir de sua entrada em vigor. Assim, é útil destacar que o tratamento de dados preexistentes deverá passar a observar a nova lei caso os dados sejam usados para novas finalidades após a entrada em vigor da nova lei.

Estamos à disposição para discutir esses itens e se precisarem de mais informações, por favor fiquem à vontade para contatar Bojana Bellamy no endereço BBellamy@hunton.com ou Markus Heyder no endereço MHeyder@hunton.com