Centre for Information Policy Leadership, Hunton & Williams LLP ("CIPL")

6 abril de 2017

PONTOS DE DISCUSSÃO

PROJETO DE LEI NO 330/2013, DO SENADO FEDERAL,

DE PROTEÇÃO DE DADOS

1. Comentários Gerais

Em termos gerais, a CIPL acredita que o projeto de lei atual inclui vários aprimoramentos significativos com relação a projetos anteriores. Por exemplo, consideramos positiva a inclusão do fundamento dos "interesses legítimos" para o tratamento dos dados, a inclusão da avaliação de risco, e assim uma abordagem com base em risco, que vemos na previsão sobre os "programas de governança em privacidade", um leque amplo de mecanismos para a transferência internacional de dados, 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. **Diferença entre responsável e operador; âmbito de aplicação da lei (Artigo 2)**

Mensagem principal: A lei deveria esclarecer sua aplicação respectivamente aos responsáveis e aos operadores, sendo a aplicação aos operadores limitada a disposições de segurança e programas de governança em privacidade (artigo 29). Além disso, a 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.

- Impor a lei de proteção de dados brasileira a responsáveis estrangeiros criaria impedimentos significativos para a indústria brasileira de serviços TI bem como para outros operadores brasileiros que prestam serviços a clientes globais. Os operadores tratam dados de clientes estrangeiros têm ser capazes de atender aos requisitos da lei estrangeira aplicável aos dados no ponto da coleta. Por exemplo, se um operador brasileiro trata dados em nome de um responsável belga, o operador brasileiro deverá ser capaz de aplicar a esses dados a respectiva lei belga – e não a lei brasileira.
- Em termos gerais, a lei deverá abranger tão somente os responsáveis localizados fora do Brasil que dirijam seus serviços especificamente a residentes brasileiros e coletem propositadamente dados pessoais de cidadãos brasileiros. Assim, acreditamos que os responsáveis estrangeiros não deveriam em geral estar subordinados à lei de proteção de dados brasileira quando os consumidores brasileiros adquiram produtos em domínios/websites não brasileiros tais como .com (em vez de .br).

3. Anonimização e Danos Anonimizados (Artigos 2 e 3)

Mensagem Principal: A legislação deveria promover o uso da anonimização dos dados como meio de reduzir riscos para os titulares. As empresas precisam de certeza jurídica de que os dados anonimizados não estão sujeitos a esta lei, e de que os dados são considerados anonimizados quando sua re-identificação somente puder ser realizada através de esforços extraordinários.

- O projeto de lei reconhece claramente a importância da anonimização e, corretamente, exclui esses dados do âmbito de aplicação da lei. O tratamento de dados anonimizados oferece diversos benefícios, tais como nas análises de *big data* para fins de pesquisa científica e aprimoramento e desenvolvimento de produtos. O projeto de lei reconhece isso, ao declarar taxativamente que essa lei não se aplica a "dados anonimizados ou dissociados".
- As disposições preveem que dados anonimizados são dados que "não podem" ser identificados por meios técnicos "razoáveis". Sugerimos que o projeto de lei defina meios técnicos "razoáveis" no sentido de que, quando esforços "extraordinários" forem necessários para re-identificar dados anonimizados, esses dados não deveriam recair no âmbito dessa lei. Além disso, sugerimos que os dados deveriam permanecer anônimos para fins dessa lei mesmo quando possam ser re-identificados por meios "razoáveis", desde que a anonimização seja acompanhada de em conjunto com proteções processuais, administrativas e legais adicionais contra a des-anonimização ou re-identificação. Assim, recomendamos que o projeto de lei também incorpore proteções processuais, administrativas e jurídicas, como, por exemplo, compromissos contratuais exequíveis com terceiros e prestadores de serviços para não re-identificar dados anonimizados, bem como as proibições legais nesse sentido. Isso irá ajudar a assegurar que dados anonimizados poderão ser reconhecidos como tal e excluídos da lei.
- Reconhecemos e entendemos que a anonimização que possa ser revertida pode representar um risco para os titulares. Por outro lado, as empresas devem ser incentivadas a anonimizar dados, pois isso reduziria o risco para os titulares. Subordinar as empresas a padrões obscuros ou de difícil cumprimento quanto a uma técnica de anonimização ser "razoável" para fins de reversibilidade ou que atenda ao nível necessário de anonimização para tirar esses dados da abrangência dessa lei não constitui incentivo para as organizações anonimizarem dados e teria pouca utilidade prática.

- Finalmente, porque às vezes a re-identificação de dados anonimizados é necessária para a prestação de certos serviços, como por exemplo na área de saúde e médica, seria útil incluir os critérios que autorizem essa re-identificação.

4. Interesse Legítimo e Consentimento (Artigo 12).

Mensagem Principal: Embora o consentimento continue sendo importante em determinadas circunstâncias, o ambiente emergente de dados e tecnologias – particularmente o chamado *big data*, a IoT e o processamento analítico – exige confiabilidade crescente no interesse legítimo como base para o tratamento dos dados.

- A CIPL ficou satisfeita de ver a inclusão dos interesses legítimos como base para o tratamento de dados. Em muitos contextos, o interesse legítimo atua como uma base de mais "responsabilização" pelo tratamento e oferece mais proteção aos titulares, visto que é necessária uma avalição e ponderação dos riscos e benefícios em cada caso, bem como a implementação de mitigações baseadas em contextos específicos.
- Todavia, conforme consta na redação, a disposição sobre os interesses legítimos não considera o critério dos interesses da sociedade. A redação atual do projeto de lei dispõe apenas que os interesses do "terceiro a quem os dados foram comunicados" poderão ser considerados. Os dispositivos típicos sobre interesses legítimos, tal como no Regulamento Geral de Proteção de Dados da União Europeia (*"EU General Data Protection Regulation –GDPR*), não incluem esse requisito de comunicação. Essa frase adicional impede uma interpretação de que o fundamento dos interesses legítimos para o tratamento também protege o interesse legítimo da sociedade, que é exatamente uma das principais considerações com relação aos vários tipos de tratamentos analíticos de *big data* mais modernos, que permitem o progresso social. Recomendamos fortemente que essa frase seja excluída.
- 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. Isso deveria constar de forma mais clara na lei.

5. **Dados Sensíveis (Artigo 15).**

Mensagem Principal: Deve-se tomar cuidado para assegurar que as disposições sobreconsentimento 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. Uma disposição sobre anonimização de dados mais clara e pragmática na forma aqui descrita poderá ajudar a resolver grande parte desse problema. Além disso, poderia ser útil permitir o tratamento de dados sensíveis com base nos interesses legítimos, nas situações onde a obtenção de consentimento expresso for impossível ou inviável.
- 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.

6. **Comunicação de Incidentes de segurança (Artigo 24)**

Mensagem Principal: Comunicação "imediata" ou "pronta" acerca da ocorrência de qualquer incidente de segurança ao órgão competente e/ou aos titulares não é uma medida realista, além de ser uma medida potencialmente danosa.

- O projeto de lei exige que o órgão competente e os titulares dos dados afetados sejam imediata ou prontamente comunicados. Trata-se de uma medida que não é realista, além de ser potencialmente contraproducente. A experiência mostra que as empresas precisam de tempo para estabelecer os fatos e a natureza da violação e para determinar quais dados foram afetados, qual o impacto e quais riscos e danos que podem resultar da violação e quais

medidas de mitigação podem e devem 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.

- A CIPL recomenda que os requisitos de qualquer comunicação sobre incidentes de segurança sejam revistos para dispor que a comunicação deve ocorrer imediatamente <u>após os fatos e a natureza da violação terem sido determinados,</u> e somente após o potencial impacto, riscos e danos aos titulares terem sido determinados (esse último ponto aparentemente já consta da redação atual do PL mas somente com relação ao dever de comunicar aos titulares).
- 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.

7. <u>Segurança (Artigo 25)</u>

<u>**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.</u>

- 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.
- Ressaltamos que essa mesma preocupação existe com relação a dados sensíveis previsto no art. 18, parágrafo único, que hoje aparentemente declara que as medidas específicas de segurança para dados sensíveis serão estabelecidas por lei.

8. Transferências Internacionais de Dados (Artigo 26)

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.
- Outrossim, acreditamos que o menu de escolhas disponíveis para as empresas deveria ser expandido. Considerando que os fluxos de dados e das atividades econômicas são hoje globais, encorajamos a inclusão de mecanismos como certificados, selos de privacidade e códigos organizacionais de conduta que são certificados por terceiros apropriados ou por uma autoridade competente. Esses mecanismos já estão sendo adotados pelo mundo. Um exemplo são as Normas Transfronteiras de Privacidade da APEC (*APEC Cross-Border Privacy Rules –CBPR),* desenvolvidas pelo fórum APEC. Outro exemplo são as Certificações da União Europeia, sob o GDPR. Acreditamos que é importante que os mecanismos de transferência de dados permitam transferências não somente dentro de um grupo empresarial global, mas também entre empresas não afiliadas. Certificados, selos e códigos de conduta reconhecidos internacionalmente apoiam esse tipo de transferência.
- 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. Programas de Governança em Privacidade e *accountability* (Artigo 29)

Mensagem Principal: A CIPL recomenda fortemente a inclusão dessa disposição sobre programas abrangentes de governança em privacidade, que assegurem o cumprimento da lei, reflitam a estrutura da organização e a natureza de suas atividades de tratamento e que incorporem boas práticas de avaliação e gerenciamento de riscos bem como a capacidade de demonstrar o cumprimento da lei como elemento principal desses programas de governança em privacidade. Além disso, deveriam existir incentivos específicos, tanto para os responsáveis quanto para os operadores, para que implementem esses programas, incluindo, por exemplo, meios de mitigação na eventual determinação e aplicação de penalidades.

- Para fortalecer e esclarecer a inclusão de avaliações de risco nesses programas, deveria ser explicado que, além de considerar o risco que o tratamento de dados traz para os titulares, as avaliações de risco devem contrabalançá-los com os benefícios potenciais do tratamento.
- Esses programas de governança em privacidade também devem incluir procedimentos para lidar com reclamações. Para evitar sobrecarregar o órgão competente e/ou o Judiciário, é importante (e possível) que a maioria das reclamações dos titulares sejam encaminhadas inicialmente ao nível da empresa.
- 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. Isso poderia ser adicionado especificamente ou esclarecido melhor na lista do Artigo 32, que disciplina os critérios para a imposição de penalidades.
- Este dispositivo também deveria esclarecer que os programas de governança em privacidade poderiam ser estabelecidos por meio de certificações ou códigos de conduta e assim também servir como mecanismos reconhecidos para transferências internacionais de dados, conforme descrito acima (vide, por exemplo, o uso pela GBPR da EU de certificações e códigos de conduta como mecanismos de transferência).

- 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.

10. Entrada em vigor e aplicação *ex nunc* (Artigo 56)

Mensagem Principal: Acreditamos que 120 dias não é um termo suficiente para as organizações implementarem os novos requisitos. Recomendamos um período de três anos para implementação da lei. Outrossim, recomendamos fortemente que esta lei seja esclarecida como tendo aplicação *ex nunc* e não retroativa (*ex tunc*), isto é, a lei não deve ser aplicável aos dados pessoais coletados antes da data de entrada em vigor da 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.
- 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.

Órgão Competente

Mensagem Principal: Um órgão ou autoridade de proteção de dados, competente e independente, é fundamental para a implementação eficaz da lei de proteção de dados no Brasil.

- Estamos preocupados com o fato de que, embora o projeto de lei faça referência a um "órgão competente", nenhuma disposição específica tenha sido incluída nesse sentido no texto. Muitas das disposições do projeto de lei não podem ser implementadas sem um "órgão competente" para servir de referência, mas o texto do projeto de lei não trata da criação dessa autoridade.
- A experiência com outras leis de proteção de dados no mundo mostra que, para essa lei ser eficaz, uma única autoridade independente de proteção de dados é essencial e deveria ser criada simultaneamente com o projeto de lei. Para assegurar consistência na interpretação e exequibilidade da lei, é importante existir uma única autoridade nacional independente, em vez de muitas autoridades competentes.
- As autoridades nacionais de proteção de dados têm papel importante na fiscalização, aplicação, interpretação, educação e cumprimento da lei nacional de proteção de dados. E, muito mais do que o Judiciário, elas têm o conhecimento necessário para interpretar a lei de proteção de dados com as nuances e a flexibilidade apropriadas em cada caso. Nesse sentido, elas ocupam um papel duplamente importante de proteger a privacidade e de permitir o melhor aproveitamento dos dados, e, assim, a era digital. Elas também têm o papel importante de ouvidoria na resolução de reclamações dos titulares. Finalmente, elas são indispensáveis para assegurar uma maior harmonia e abordagem consistente com regulamentos de proteção de dados de outros países. As autoridades nacionais de proteção de dados trabalham muito próximas entre si através de organizações regionais e internacionais como o *Interrnational Conference of Data Protection and Privacy Commissioners (ICDPPC),* a rede *Ibero-American Data Protection Network (RIPD)*, a *APEC Cross-border Privacy Enforcement Arrangement (CPEA)* e a rede *Global Privacy Enforcement Network (GDPR)*. É vital que o Brasil seja representado nessas organizações através de uma autoridade nacional de proteção de dados.

.

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