25 de agosto de 2017

**RESPOSTA DO *CENTRE FOR INFORMATION POLICY LEADERSHIP***
CONSULTA PÚBLICA SOBRE A ESTRATÉGIA BRASILEIRA PARA A TRANSFORMAÇÃO DIGITAL

O *Centre for Information Policy Leadership de Hunton & Williams LLP* (CIPL)[1] tem o prazer de responder ao Ministério da Ciência, Tecnologia, Inovações e Comunicações do Brasil (MCTIC) em sua iniciativa de desenvolver a Estratégia Brasileira para a Transformação Digital (a "Estratégia"). Enquanto a Estratégia lida com vários temas, a resposta do CIPL diz respeito essencialmente ao aspecto da confiança no ambiente digital. O CIPL acredita que ter uma autoridade única, nacional e independente de proteção de dados é essencial para um ambiente digital seguro e confiável. A designação de tal autoridade nacional responsável pela proteção de dados pessoais assegura proteção eficaz de privacidade para indivíduos, uso consciente e responsável de informações pessoais por empresas, a promoção de melhores práticas com relação ao uso de informações pessoais, relacionamento eficaz com autoridades globais de proteção de dados (APDs) sobre política de privacidade e assuntos de cooperação para fiscalização e é essencial para possibilitar a existência da moderna economia de dados e inovação.

## 1. Designação e Objetivos de uma Autoridade Central de Proteção de Dados

A confiança no ambiente digital pode ser promovida pela designação de uma autoridade de proteção de dados (APD) central e independente. É importante haver uma única autoridade competente central em vez de múltiplas autoridades competentes por várias razões. A experiência com outras leis de proteção de dados e com sua aplicação ao redor do mundo demonstra que uma autoridade central garante:

- Consistência na interpretação e aplicação da lei de proteção de dados;
- Uniformização das recomendações, ações educativas e orientações sobre questões de proteção de dados;
- Procedimentos consistentes na fiscalização do cumprimento da lei;

[1] CIPL (Centro para a Liderança em Políticas de Informação) é um laboratório de ideias do escritório jurídico Hunton & Williams LLP para a proteção da privacidade e da proteção de dados, e é apoiado financeiramente pelo escritório jurídico e por 54 empresas afiliadas, líderes em setores-chave da economia global. A missão do CIPL é engajar-se na liderança do pensamento e no desenvolvimento de melhores práticas para assegurar a proteção eficaz e o uso eficaz e responsável de informações pessoais na atual era da informação. Para mais informações, acesse o sítio do CIPL em http://www.informationpolicycentre.com/. Nenhuma parte deste conteúdo deverá ser entendida como representativa do ponto de vista individual de qualquer empresa afiliada ao CIPL ou do escritório jurídico Hunton & Williams.

- Padrões uniformes e melhores práticas para empresas;

- Evitar a escolha de um foro favorável (*forum shopping*) por consumidores que apresentam reclamações ou por empresas que enfrentam sanções por não cumprimento, práticas desleais ou enganosas ou outros comportamentos não aceitáveis;

- Harmonização da proteção de dados transfronteiriça com outros países;

- Um ponto de contato com organizações regionais e internacionais tais como a Conferência Internacional dos Comissários para a Proteção de Dados e Privacidade (*International Conference of Data Protection and Privacy Commissioners*- ICDPPC), a Rede Ibero-americana de Proteção de Dados (*Ibero-American Data Protection Network* - RPID), Autoridades de Privacidade da Região Ásia-Pacífico (*Asia Pacific Privacy Authorities* -APPA), o Arranjo Transfronteiriço para a Garantia da Privacidade (*Cross-border Privacy Enforcement Arrangement* - CPEA) da Cooperação Econômica da região Ásia-Pacífico (*Asia-Pacific Economic Cooperation* - APEC), a Rede Global para Aplicação da Legislação sobre a Privacidade (*Global Privacy Enforcement Network* - GPEN) e outras.

- Um ponto de contato para APDs internacionais para questões transfronteiriças de aplicação da lei; e

- Uma agenda nacional (que considere os pontos de vista de todas as partes interessadas) para o desenvolvimento de regras e boas práticas sobre proteção de dados, livre da competição de múltiplas agendas propostas por diversas autoridades.

Uma autoridade central "especializada" irá representar o Brasil em assuntos de proteção de dados com uma só voz tanto a nível nacional como internacional. Sua missão será de manter-se atualizada sobre o desenvolvimento tecnológico, práticas de negócios e temas de privacidade relevantes, e implementar medidas que possam abordar de forma prática e eficaz as questões e ao mesmo tempo garantir o avanço da inovação tecnológica e o crescimento do mercado digital. Em escala internacional, a autoridade central falará em nome do Brasil sobre aspectos e ações de política global de proteção de dados e cooperará com as autoridades que representem seus equivalentes estrangeiros em assuntos transfronteiriços de aplicação da lei de privacidade. Múltiplas autoridades nacionais com competência concorrente sobre proteção de dados, a despeito de suas boas intenções, não conseguem atingir tais objetivos. Designar uma autoridade competente única garantirá uma liderança forte, flexibilidade e, o que é mais importante, a confiança no ambiente digital brasileiro. Além disso, esta autoridade central deve ser funcional e operacionalmente independente do governo, particularmente com relação às suas investigações, decisões sobre aplicação da lei, liderança e assuntos de recursos humanos, dado que tal independência é um critério relevante para afiliação e participação eficaz em certas organizações globais de autoridades de proteção de dados (APDs), tais como a ICDPPC.

## 2. Garantindo a Eficácia da APD Central

A confiança no ambiente digital pode ser aumentada pela designação de uma APD competente única, desde que esta APD tenha um papel claro e que possa ser desempenhado de forma eficaz. Maximizar a eficácia de APDs é uma tarefa complexa. Suas funções são numerosas, as expectativas são altas e os recursos tendem a ser escassos. As APDs não podem fazer tudo e, portanto, precisam fazer escolhas difíceis porém essenciais sobre estratégias e prioridades. As APDs também precisam adotar abordagens modernas e estratégicas com relação à regulamentação com vistas a obter os melhores resultados para os indivíduos, a sociedade e organizações regulamentadas. Isto implica no engajamento de forma responsável e no apoio a negócios que buscam adotar as melhores práticas no tratamento de dados pessoais, e ao mesmo tempo atuar de maneira firme em relação àqueles que não buscam fazer o mesmo. O CIPL define esta abordagem como uma abordagem baseada em resultados.

Os fundamentos de uma abordagem baseada em resultados podem ser resumidos pelos seguintes princípios gerais:

- A regulamentação para resultados requer uma APD independente para que sua atuação seja estratégica, eficaz, coordenada e transparente;

- A APD deverá ser capaz de produzir resultados por meio de uma boa relação custo-benefício, que protejam os indivíduos na prática, promova o tratamento consciente dos dados e facilite a prosperidade e inovação;

- A APD deverá considerar como absoluta prioridade assegurar a proteção dos indivíduos;

- A APD deverá detalhar de forma transparente os resultados esperados e as prioridades e abordagens que serão utilizadas para a consecução de seus objetivos;

- A APD deverá ser capaz de colaborar e coordenar políticas que garantam a aplicação da lei de proteção de dados nacional com abordagens junto a APDs estrangeiras equivalentes, para a melhoria da consistência em uma economia de dados global, na medida do possível.

- A APD deverá tratar as organizações regulamentadas de forma consistente - adotando abordagens semelhantes em cada setor e entre setores;

- A APD deverá adotar uma abordagem de avaliação de risco em todas as suas atividades, baseando suas políticas e voltando a prioridade da sua atuação para as condutas que criem os maiores prejuízos aos indivíduos ou a valores democráticos e sociais;

- A ADP deverá adotar uma abordagem de engajamento construtivo com a indústria, com ênfase em liderança, informação, orientação, diálogo e apoio, no lugar da dependência excessiva a ações de restrição e punição;

- A APD deverá estimular relações abertas e construtivas com negócios que lidem com dados pessoais, com base em diálogo franco e cooperação mútua, com responsabilidades claras;

- As organizações regulamentadas deverão ser avaliadas principalmente com base na boa-fé e em auditoria prévia em seus esforços para cumprir a lei;

- Organizações que estejam empenhadas em agir de forma responsável deverão ser encorajadas a identificar-se proativamente com base no princípio da *accountability*, por exemplo, conduzindo de forma transparente processos de prestação de contas, implementando programas de privacidade e gerenciamento de risco, buscando o reconhecimento de suas boas práticas por meio de selos e programas de certificação, códigos de conduta, Normas Corporativas Vinculantes (*Binding Corporate Rules* - BCR), Regras Transfronteiriças da APEC de Proteção à Privacidade (APEC Cross-Border Privacy Rules (CBPR)) e outros padrões de *accountability*;

- Sanções e punições deverão ser dirigidas principalmente a atividades que violem a lei de proteção de dados de forma deliberada e intencional, por meio de práticas seriamente negligentes, repetidas ou particularmente graves;

- As reclamações deverão ser gerenciadas de maneira firme pois podem desviar a atenção de atividades mais estratégicas das APDs, e podem consumir muitos de seus recursos. Não deve haver exigência de investigação de toda e qualquer reclamação; em vez disso, as APDs deverão ter liberdade de escolher quais casos irão investigar cuidadosamente, ao mesmo tempo tendo em conta que reclamações são uma importante fonte de informação.

## 3. <u>Potenciais Desafios para uma Autoridade Nacional em Proteção de Dados</u>

Existem desafios específicos tipicamente associados à designação de uma autoridade nacional para a proteção de dados, que devem ser considerados e tratados. Esses incluem a provisão de recursos adequados para as APDs e a superação do ceticismo dos regulamentados, enquanto buscam os níveis e modos apropriados de se relacionar de forma construtiva com aqueles mesmos entes regulamentados, entre outros.

- **Provisão de recursos adequados para as APDs**: de forma a desempenhar suas tarefas de forma eficaz, as APDs precisam ter recursos apropriados. A pesquisa mais recente de orçamentos de APDs foi conduzida como um censo pelo ICDPPC em 2017.[2] Para 26

[2] Os dados do censo estão disponíveis mediante solicitação à Conferência Internacional dos Comissários para a Proteção de Dados e Privacidade (*International Conference of Data Protection and Privacy Commissioners Secretariat*), https://icdppc.org/the-conference-and-executive-committee/icdppc-census/.

países da União Europeia[3] que forneceram dados, o orçamento total para essas autoridades em 2016 foi de €205.703.574 para uma população total naquele ano de 507.471.970.[4] Isto sugere que, no total desses 26 países, o orçamento por cidadão foi menor que €0,41. Isto representa muito pouco e demonstra como são limitados os recursos para cada APD. Entendemos, contudo, que um aumento significativo de orçamento está sendo implementado ou seriamente considerado em diferentes países da União Europeia. Para assegurar a eficácia de sua APD e ao mesmo tempo promover a confiança no ambiente digital, o Brasil deverá garantir a provisão de recursos financeiros adequados e levar em conta sua APD na proposta anual de orçamento. Algumas APDs já recebem receita por serviços remunerados tais como auditoria, treinamento e publicações. As APDs devem tentar a todo custo evitar financiar suas atividades aplicando multas por não cumprimento daqueles a quem regula. Qualquer tentativa deste tipo será altamente controversa e sujeita a contestações éticas, políticas e legais. Uma possível fonte de renda pode ser a cobrança de taxa modesta anual de todas as organizações que processam dados pessoais (na verdade, provavelmente todas as empresas e órgãos públicos). Considerando o tamanho do Brasil e o número de empresas regulamentadas, uma taxa de somente 75 reais geraria milhões em receita para ajudar a APD a exercer suas funções de forma eficaz. Uma APD com bom nível de recursos passa ao público a confiança que seu direito à proteção de dados está protegido por uma organização que tem os meios para fazê-lo.

- **Ceticismo dos regulamentados**: como o Brasil não tem atualmente uma autoridade nacional de proteção de dados, pode haver alguma resistência em trabalhar com a APD por aqueles a quem a autoridade vai regular. Embora o engajamento com as empresas regulamentadas seja essencial e deva ser promovido, já que constitui um dos aspectos de eficácia das APDs, algumas empresas regulamentadas podem estar inclinadas a manter distância de uma APD por receio de receber punições por má conduta no passado, ter documentos ou práticas disponibilizadas para a APD durante as consultas que possam ser utilizados contra a empresa em questões relativas a cumprimento da lei, ou receio de veto a alguma inovação planejada. Para evitar este risco, a APD deve se empenhar para estabelecer uma relação de confiança mútua com as organizações regulamentadas e promover um ambiente de apoio e colaboração. Isto vai gerar confiança no ambiente digital para as empresas.

## Conclusão

Esperamos que o conteúdo acima forneça um esclarecimento útil sobre a forma como o Brasil pode promover a confiança no ambiente digital e como adaptar sua estratégia sobre transformação digital. O presente comentário representa um breve resumo de um artigo intitulado "Regulamentação para Resultados no Mundo Digital: Estratégias e Prioridades para

[3] Valores não disponíveis para Áustria ou Croácia, e os valores da Alemanha são mais baixos que o valor real, pois somente 7 dos 16 estados forneceram dados.

[4] Dados de população para os 26 estados relevantes da União Europeia foram obtidos do Banco Mundial em 27 de julho de 2017, http://data.worldbank.org/indicator/SP.POP.TOTL.

Liderança e Engajamento (*Regulating for Results in the Digital World: Strategies and Priorities for Leadership and Engagement*)", que o CIPL vai lançar na 39ª Conferência Internacional dos Comissários para a Proteção de Dados e Privacidade (*International Conference of Data Protection and Privacy Commissioners*) em Hong Kong, em setembro de 2017. Vamos disponibilizar este artigo para vocês quando estiver publicado, dando continuidade a este comentário para elaboração mais profunda dos pontos acima. Gostaríamos também de discutir quaisquer aspectos de nosso pensamento que possam especificamente auxiliar a iniciativa brasileira.

Para a discussão de quaisquer desses temas mais a fundo, ou para solicitar informações adicionais, favor entrar em contato com Bojana Bellamy, bbellamy@hunton.com, Markus Heyder, mheyder@hunton.com ou Sam Grogan, sgrogan@hunton.com.