PEC sobre proteção de dados pessoais

Camara dos deputados – Audiencia pública

Brasilia, 26 de novembro de 2019

Prezada Deputada Bruna Furlan, Presidente da Comissão Especial destinada a proferir parecer à Proposta de Emenda à Constituição nº 17 de 2019.

Prezado Deputado Orlando Silva, Relator da Proposta de Emenda à Constituição nº 17 de 2019 nesta Comissão Especial.

Prezado Carlos Bruno Ferreira da Silva, Procurador da República,

Prezada Bojana Bellamy, Representante do Centre for Information Policy Leadership - CIPL;

Senhoras e Senhores Deputados

Senhores e Senhoras,

Em primeiro lugar, quero agradecer o amável convite e a oportunidade concedida à União Europeia de contribuir no âmbito desta importante audiência pública em um momento tão importante para a proteção de dados no Brasil.

Com a adoção, no ano passado, da Lei Geral de Proteção de Dados Pessoais (LGPD), o Brasil figura com destaque no mapa mundial de privacidade. É também para a UE um parceiro importante nessa área. Parabenizamos o trabalho que vem sendo feito pelo Congresso brasileiro nesse âmbito. O trabalho em andamento diante desta Câmara sobre o projeto de lei que adiciona a proteção de dados como um direito fundamental à Constituição Brasileira é mais uma expressão de sua liderança e um exemplo para muitos países nesta região e além dela.

Permitam-me, portanto, dizer algumas palavras sobre esses acontecimentos recentes, bem como sobre as perspectivas de fortalecer a parceria UE-Brasil na área de proteção de dados e fluxos de dados. Isso também me permitirá compartilhar com vocês algumas lições aprendidas na Europa decorrente da aplicação da nossa nova legislação, o Regulamento Geral de Proteção de Dados (conhecido como “GDPR”), pois essas tendências podem ser de interesse no contexto de suas discussões.

Compartilhamos **os mesmos valores e uma visão comum** em relação às oportunidades e desafios em torno do uso de dados pessoais.

Acreditamos que, no mundo de hoje, mais do que nunca, o direito fundamental a privacidade precisa ser efetivamente protegida. Isso significa uma legislação abrangente, com base em um conjunto principal de direitos individuais e implementado por um regulador forte.

É uma **questão de direitos individuais**, reconhecidos por nossas respectivas estruturas constitucionais. É, e cada vez mais, um **imperativo democrático**, em um momento em que o uso indevido de dados pode afetar a integridade do processo eleitoral e, portanto, o próprio funcionamento de nossa democracia. É também uma **necessidade econômica**. Sem a confiança dos consumidores na maneira como seus dados são tratados, não pode haver crescimento sustentável de nossa economia cada vez mais orientada pelos dados.

É por isso que, no Brasil e na UE, adotamos regras modernas de proteção de dados como um componente central de nossas respectivas estratégias digitais. Essa reflexão também se encontra ao nível global, onde alguns princípios importantes de privacidade (como prestação de contas, transparência, explicabilidade, capacidade de desafio) são reconhecidos mais amplamente como parte integrante de uma abordagem humanocêntrica muito necessária da Inteligência Artificial - como refletido, por exemplo, nos Princípios da OCDE sobre Inteligência Artificial, adotados há alguns meses.

Na Europa, estamos já vendo os efeitos positivos dessa escolha.

Embora seja normal, como para qualquer legislação importante, que o GDPR tenha exigido adaptações para podermos implementar às novas regras, nenhum dos cenários qualificados de "desgraça e melancolia" e que estávamos ouvindo antes da nova lei entrar em vigor se materializou.

A **harmonização** é um primeiro benefício tangível da implemetação do GDPR, que foi bem recebida por todas as nossas partes interessadas, da sociedade civil à comunidade empresarial. Ficou claro para nós que precisávamos de legislação no nível da União Europeia (o equivalente ao seu nível federal). Ao lidar com atividades de processamento de dados, que claramente não param nas fronteiras físicas, não fazia sentido ter na Europa um quadro regulamentar fragmentado composto por 28 legislações diferentes.

Essa harmonização é essencial para os cidadãos, os consumidores e as empresas. Significa um nível consistente de proteção em toda a União Europeia, a garantia de um direito fundamental que não varia de um Estado membro para o outro. Por exemplo, para as empresas, isso significa regras comuns do jogo, garantindo que os dados

possam circular facilmente pelo continente, entre setores ou modelos de negócios, entre o setor público e o privado etc., sem custos adicionais de conformidade. Isso é particularmente importante para empresas de menor porte que tanto na União Europeia como no Brasil são a espinha dorsal da nossa economia.

O que também ouvimos das empresas na Europa é que a aplicação do GDPR foi, em primeiro lugar, uma oportunidade de **colocar o seu "data house" em ordem**, analisando com mais atenção o tipo de dados coletam, as finalidades de uso, como eles são conservados, se são compartilhados e, não menos importante, se eles realmente precisam coletar e processar todos esses dados.

A resposta a essas perguntas muitas vezes tem permitido as empresas **reduzir a exposição a riscos desnecessários. De fato,**: por exemplo, em um relatório recente da empresa multinacional de tecnologia Cisco, a implementação do GDPR levou as empresas a estarem mais bem preparadas para evitar infracções relativas a segurança e serem mais responsivas em caso de incidente que lhes permita mitigar as consequências de tais incidentes. Isso é de suma importância hoje em dia, se considerarmos as perdas financeiras e/ou danos à reputação que essas infracções podem causar, como por exemplo no recente rebaixamento da Moody's da empresa americana

de relatórios de crédito Equifax, após um grande incidente de segurança de dados.

Responder a essas perguntas geralmente também permite que as empresas tenham uma ideia melhor de quais dados elas preservam e como "explorá-los" melhor, desenvolvendo um **relacionamento mais confiável com seus clientes e parceiros comerciais**.

Na realidade, a implementação do GDPR mostrou o que é realmente a proteção de dados, ou seja, o “simples” gerenciamento de dados. Trata-se principalmente de ter uma cultura de uso responsável dos dados, estabelecendo regras operacionais para aqueles que lidam em todos os níveis com dados e garantindo a segurança apropriada desses mesmos.

O que também vemos é que a proteção de dados é cada vez mais um **diferencial de venda**, à medida que cada vez mais usuários (no contexto B2B ou B2C) valorizam a privacidade e a segurança de seus dados. Por exemplo, estamos observando no mercado a oferta de produtos inovadores e serviços com soluções inovadoras de privacidade ou segurança. Muitas empresas declaram que a privacidade está se tornando cada vez mais um diferencial competitivo em seus mercados.

Esses progressos não se limitam à União Europeia, mas também dizem respeito a economias estrangeiras muito inovadoras. Para mencionar apenas um exemplo, Israel, que é frequentemente chamada de "nação start-up": de acordo com um relatório publicado pela associação de segurança cibernética de Israel em 2018, o subsetor de proteção de dados e privacidade foi um nicho de crescimento mais rápido nessa indústria, pelo menos em parte como resultado da entrada em vigor do GDPR.

Estou mencionando tais aspectos porque esses são benefícios que **vão muito além de “apenas” cumprir os requisitos legais e regulatórios**.

Um dos objectivos principais do GDPR foi de dar aos indivíduos um controle maior sobre os dados. Isto é claramente um longo processo e que não só depende das leis applicáveis. Estamos vendo uma consciência mais ampla dos cidadães sobre os seus direitos a privacidade. Isso é um sinal encorajador, pois indivíduos mais bem informados estão cada vez mais usando seus direitos e considerando aspectos de privacidade ao tomar certas decisões. Como União Europeia, nós acreditamos que é importante expandir ainda mais a conscientização dos cidadãos nesse campo. E é por isso que nós por

exemplo lançamos recentemente uma campanha para encorajar os cidadãos a otimizar suas configurações de privacidade.

O que este primeiro ano e meio também mostrou claramente é quanto crucial é o papel desempenhado por órgões reguladores independentes (autoridades de proteção de dados) que contribuiem para uma implementação bem-sucedida da lei.

Em particular, o que nossa experiência nos diz é que, em um campo em rápida evolução como o de processamento de dados e considerando que qualquer lei de privacidade precisa necessariamente permanecer em um certo nível de abrangência, a orientação de um regulador confiável e independente permite adaptar a aplicação da legislação a novos desenvolvimentos tecnológicos e econômicos.

Foi o que aconteceu na UE: desde maio de 2018, as autoridades europeias de proteção de dados (trabalhando juntas no âmbito do "Comitê Europeu de Proteção de Dados") se envolveram construtivamente com as partes interessadas, com o entendimento de que a **conformidade é um processo dinâmico**.

É nisso que nossas autoridades de proteção de dados se concentram. Isso resultou notavelmente na emissão de mais de 20

diretrizes detalhadas nos últimos dois anos, aprofundando os novos aspectos do GDPR. Cada um desses conjuntos de diretrizes foi adotado após consulta pública.

Também foram desenvolvidas ferramentas específicas para atender às necessidades específicas de pequenas e médias empresas e start-ups, além de apoiar a inovação favorável à privacidade. Nos próximos meses, haverá mais novidades para abordar a aplicação das regras de proteção de dados em áreas em rápida evolução, como carros blockchain ou conectados/autônomos.

E quando as sanções são promulgadas, isso tem sido sempre, é claro, no seguimento de uma investigação completa dos fatos do caso e com base nas circunstâncias específicas do caso (gravidade, duração, impacto nos indivíduos, peso econômico da empresa em questão etc.). Podemos ver isso refletido por exemplo na variação dos valores das primeiras multas aplicadas: dos 5.000 euros (o equivalente a aproximadamente 23.000 reais) a um café de apostas esportivas por videovigilância ilegal até a multa de 50 milhões de euros (aproximadamente 230 milhões de reais) à Google em um caso referente às condições sob as quais obteve consentimento para determinadas operações de processamento. Em outros casos, não foi aplicada qualquer multa, mas foi emitido um aviso ou advertência.

Acreditamos que a melhor multa é na realidade a que nunca é imposta, mas, ao mesmo tempo, nossa experiência nos diz que, se você deseja que as regras de privacidade sejam levadas a sério, você precisa de mecanismos de aplicação críveis e sanções suficientemente dissuasivas.

O papel das autoridades de proteção de dados se tornará ainda mais significativo, pois há uma clara necessidade de mais cooperação e assistência mútua entre os garantidores de privacidade, no momento em que eles precisam cada vez mais lidar com problemas ou incidentes de conformidade semelhantes que afetam simultaneamente os cidadãos de múltiplas jurisdições. Essa cooperação, por meio do desenvolvimento de ferramentas interpretativas comuns ou do intercâmbio de melhores práticas, também pode contribuir para garantir um ambiente jurídico mais claro para as empresas que operam em várias jurisdições.

Por todos esses motivos, estamos **ansiosos para trabalhar em estreita colaboração com a Autoridade Nacional de Proteção de Dados (ANPD)** que está sendo criada atualmente.

Em um momento em que há uma demanda crescente por padrões internacionais e cooperação nessa área, é muito importante que o

Brasil possa contribuir plenamente para o seu desenvolvimento, através da voz oficial e do conhecimento de sua entidade de proteção de dados.

Isso me leva ao último ponto que eu queria mencionar: **convergência global** nos padrões de privacidade.

Hoje, uma coisa é clara: a convergência sobre a privacidade é real, está acontecendo diante de nossos olhos. Os principais componentes de uma estrutura moderna de privacidade, à qual eu estava me referindo anteriormente: uma legislação abrangente, um conjunto principal de direitos aplicáveis, um regulador forte, são cada vez mais compartilhados globalmente, do Brasil ao Japão, do Chile à Coréia do Sul, do Quênia à Indonésia ou Tailândia.

De fato, em um mundo que muitas vezes é caracterizado por fragmentação, por abordagens diferentes, se não divergentes, essa tendência à convergência global é um desenvolvimento positivo que traz novas oportunidades para aumentar a proteção dos indivíduos quando seus dados circulam, mas também para facilitar o fluxo de dados e, portanto, comercial (bem como cooperação entre autoridades públicas). Em outras palavras, **a convergência em**

privacidade compensa. Esta é uma situação em que todos saem ganhando, tanto consumidores quanto empresas.

Isso não exige, ao contrário do que às vezes ouvimos, sistemas de harmonização para torná-los idênticos (pois refletem naturalmente diferentes tradições legais, culturas, escolhas sociais etc.). Trata-se, sim, de desenvolver os principais pontos em comum.

O acordo de adequação mútua União Europeia-Japão recentemente concluído, que estabelece a maior área do mundo de fluxos de dados gratuitos e seguros, ilustra esse ponto. Os resultados desse acordo foram imediatos e muito benéficos para as duas economias: desde fevereiro, os dados podem fluir livremente entre a UE e o Japão e entre o Japão e a UE sem a necessidade de autorizações, contratos sofisticados, certificação ou outros mecanismos dispendiosos. Isso é particularmente vantajoso para empresas menores.

Ao permitir o fluxo livre de dados, esse acordo também ampliou os benefícios do acordo de livre comércio recentemente concluído entre o Japão e a UE, já que o comércio depende cada vez mais do intercâmbio de dados. Isso mostra como instrumentos comerciais e mecanismos de proteção de dados podem se complementar.

A convergência nos padrões de privacidade traz, portanto, benefícios muito tangíveis em termos de vantagem competitiva, acesso ao mercado e oportunidades de negócios. Isso se tornou ainda mais relevante para nossas respectivas economias e nosso comércio bilateral após a recente conclusão do Acordo de Associação UE-Mercosul.

Como União Europeia, estamos comprometidos em intensificar nosso compromisso com as autoridades brasileiras para desenvolver essas sinergias entre ferramentas comerciais e de proteção de dados. A adoção do GDPR e da LGPD, o reconhecimento da proteção de dados como um direito fundamental e a criação da ANPD vão aproximar muito nossos sistemas de privacidade. Poderíamos aproveitar essa convergência em vista de adquirir um nível de adequação, que garantiria o fluxo livre e desimpedido de dados entre a UE e o Brasil.

Como vocês podem ver, provavelmente estaremos muito ocupados trabalhando juntos nos próximos meses e anos. E é assim que deve ser se queremos abordar desafios e oportunidades cada vez mais globais em natureza e escopo.

Portanto, com isso tudo em mente, estamos acompanhando com grande interesse o atual debate sobre proteção de dados pessoais no Brasil. Eu gostaria, enfim, de agradecer novamente pelo convite e pela oportunidade que foi dada para compartilhar algumas ideias e experiências. E permitam-me enfatizar, em nome da União Europeia, o quanto nós valorizamos o diálogo, que espero que possa continuar e progredir nos próximos meses. Foi uma grande honra participar em nome do meu colega Bruno Gencarelli, Diretor da Unidade Internacional de Proteção de Fluxos de Dados da Comissão Europeia. Convidamos a enviar suas consultas técnicas por escrito. Será um prazer dar continuidade a este diálogo.

Obrigado pela atenção!