Ao Ministério da Justiça
Esplanada dos Ministérios, Palácio da Justiça, Bloco T, Edifício sede.
CEP 70064-900 - Brasília-DF

São Paulo, julho de 2015.

RE: contribuições do IAB Brasil ao Debate Público do Anteprojeto de Lei de Proteção de Dados Pessoais

1) Sobre o IAB Brasil

O Interactive Advertising Bureau (IAB) foi fundado em 1998, com a principal missão de desenvolver o mercado de mídia interativa no Brasil. A partir de 2006, a Associação de Mídia Interativa (AMI) passou a fazer parte da mais importante rede de associações do mundo – O Interactive Advertising Bureau, mudando sua denominação para IAB Brasil. Desde então, a associação integra uma rede internacional de associações, que conta com representações em mais de 45 países, entre eles EUA, Austrália, Cingapura, Espanha, França, Inglaterra, Itália, Chile e México.

O IAB Brasil conta atualmente com mais de 220 filiados, entre sites, portais, empresas de tecnologia, agências e desenvolvedoras Web, líderes em seu segmento no país.

O IAB Brasil é uma entidade sem fins lucrativos que tem como missão:

- incentivar a criação de normas e padrões para o planejamento, criação, compra, venda, veiculação e mensuração de mensagens comerciais;
- desenvolver o intercâmbio, em nível nacional e internacional, por meio de cursos, palestras e publicações, de experiências e conhecimentos técnicos de seus associados;
- regulamentar as pesquisas e estudos que comprovem a eficiência da mídia interativa;
- promover a identificação de oportunidades de posicionamento da mídia interativa através de linguagem publicitária para atrair o interesse de anunciantes e profissionais da mídia tradicional.

Entende-se por meios interativos a rede mundial de computadores (Internet), a TV Interativa, as plataformas para envio de mensagens comerciais por telefones celulares e aparelhos de mão portáteis (“PDAS”), bem como os novos canais de comunicação que venham a surgir a partir do avanço da tecnologia e que permitam a publicação ou envio de mensagens comerciais com características semelhantes às atuais.

Mais informações sobre o IAB Brasil estão disponíveis no web site http://iabbrasil.net/portal/.

2) Considerações Iniciais

O IAB BRASIL entende fundamental relembrar que é a publicidade dirigida, possibilitada pelo tratamento de dados de usuários – pessoais ou não – que sustenta o ecossistema de serviços e de informações gratuitas online. O acordo entre as partes onde uma delas autoriza o tratamento de seus dados em troca da utilização de serviços é uma escolha válida e precisa ser respeitada.

Cumpre ressaltar que é perfeitamente lícito e válido dentro do ordenamento jurídico brasileiro (e sequer uma novidade, vale notar) o contrato bilateral e sinalagmático de permuta – que é exatamente o modelo aplicável à maioria das situações vivenciadas hoje na Internet, no qual usuários acessam determinados serviços em troca da autorização do tratamento de seus dados pessoais.

É esse modelo que permite a todos os usuários participar do ecossistema online, e não apenas a quem dispõe de recursos para pagar por conteúdo e serviços. Dificultar o tratamento de dados para fins comerciais pode inviabilizar práticas lícitas consagradas no mercado brasileiro e emperrar a economia digital.

Evidentemente, isso não significa que usuários não devam ter controle algum sobre seus dados pessoais – consumidores devem ser adequadamente informados de quais concessões fazem e que trocas aceitam quando optam por usar serviços e acessar conteúdo gratuito online, bem como devem ter acesso a ferramentas que viabilizem

esse tipo de controle nas plataformas digitais, redes sociais e demais serviços online que utilizam.

Com base nessas premissas, o IAB Brasil apresenta, a seguir, suas contribuições ao anteprojeto de lei de proteção de dados pessoais (APL):

a) Aplicação da Lei e "Órgão Competente"

Leis gerais de proteção de dados pessoais têm a difícil missão de equilibrar a inovação baseada em dados com a proteção do cidadão contra potenciais danos. Tais leis costumam apresentar uma redação baseada em princípios gerais, de modo a permitir interpretações adequadas à realidade de um determinado momento.

Em razão dos constantes avanços tecnológicos, o papel do intérprete de leis gerais de proteção de dados torna-se ainda mais crucial, ao assegurar que a aplicação da lei acompanhe a velocidade das inovações ao longo do tempo. A experiência internacional evidencia que diretrizes claras trazem segurança jurídica e asseguram que as inovações observem a necessária proteção dos direitos do cidadão, ao passo que interpretações imprecisas geram incertezas que podem dificultar ou até mesmo inviabilizar atividades empresariais legítimas sem proteger efetivamente o cidadão contra potenciais danos.

Nesse ponto, o APL menciona que caberá a um "órgão competente" uma grande variedade de atribuições essenciais com o objetivo de interpretar, fiscalizar e fazer cumprir a lei de proteção de dados pessoais.

O APL não define, porém, qual seria esse órgão competente, nem menciona qual seria sua estrutura ou composição. Não está claro, portanto, se essas atribuições essenciais seriam delegadas a diversos órgãos já existentes, ou a um único órgão federal já existente; ou, ainda, se haveria a criação de um órgão específico para a proteção de dados pessoais. **Entendemos que o anteprojeto de lei deve definir qual será esse órgão competente, de forma a se evitar insegurança jurídica e para que a sociedade saiba quem terá o papel de interpretar, fiscalizar e fazer cumprir a lei.**

b) Jurisdição

O IAB Brasil entende que o âmbito de aplicação do APL é excessivamente amplo, pois pretende regular atividades de tratamento de dados pessoais de qualquer pessoa que esteja no Brasil, afastando-se da legislação comparada a respeito do assunto.

Tendo em vista a vasta abrangência do conceito de tratamento previsto no APL, e os possíveis impactos negativos que tal conceito abrangente pode trazer para o simples trânsito de dados pelo território nacional, sugere-se que o APL passe a trazer de maneira clara, como uma exclusão da aplicação do escopo da lei, a situação de dados que circulem de maneira meramente transitória pelo território nacional.

Imagine-se, por exemplo, dados que sejam coletados na Itália, que serão tratados no Uruguai, e que simplesmente trafeguem pelo território brasileiro no caminho. Não parece fazer sentido aplicar a legislação brasileira a esses dados, ainda que algumas das operações definidas pelo APL como hipótese de tratamento tenham ocorrido.

Sugere-se, assim, que o APL mencione expressamente que a lei não se aplica a dados que estejam meramente em trânsito, evitando-se com isso conflitos de jurisdições.

c) Conceito de dado pessoal

O texto do APL adota um conceito extremamente amplo de dado pessoal, mencionando que é considerado dado pessoal o *"dado relacionado à pessoa natural identificada ou identificável, inclusive a partir de números identificativos, dados locacionais ou identificadores eletrônicos"*.

Tal como redigido, o conceito engloba dados que não identificam uma pessoa natural, mas que estão meramente "relacionados" a ela. Com isso, ficariam sujeitos à lei praticamente todos os dados produzidos pela atividade humana, ainda que não possam ser razoavelmente utilizados para identificar esse titular.

Um conceito mais preciso é adotado pela legislação do Canadá - “dados sobre uma pessoa natural”, e se mostrou mais adequado para equilibrar a proteção do titular com o livre fluxo de informações.

Nas discussões mais recentes sobre o tema no âmbito da regulação geral de proteção de dados na Europa (GDPR), têm-se sugerido que o conceito de dados pessoais seja revisado para englobar somente dados que razoavelmente permitam a identificação de uma pessoa natural, excluindo-se do conceito todos os dados que não sejam efetivamente capazes de identificar razoavelmente um indivíduo, bem como todos os dados que passarem por processos de anonimização.

Sugere-se, assim, que o conceito de dado pessoal previsto no artigo 5º, inciso I do APL seja modificado, mencionando-se que dado pessoal é o *“dado que identifique ou permita, por meios razoáveis, a efetiva identificação da pessoa natural”.*

d) Dados anônimos: conceito e aplicação prática

O APL conceitua dados anônimos no artigo 5º, inciso IV, como *“dados relativos a um titular que não possa ser identificado, nem pelo responsável pelo tratamento nem por qualquer outra pessoa, tendo em conta o conjunto de meios suscetíveis de serem razoavelmente utilizados para identificar o referido titular”.*

Apesar de conceituar dados anônimos, o APL não volta a mencionar a expressão em nenhum outro ponto do texto. Para maior clareza, seria imprescindível observar que a) o tratamento de dados anônimos está fora do âmbito de aplicação da lei e, justamente por isso, b) o tratamento de dados anônimos pode ser efetuado sem quaisquer exigências ou formalidades.

Sugere-se, assim, a inclusão de inciso III ao parágrafo 2º do artigo 2º, para deixar claro que a lei não se aplica ao tratamento de dados anônimos, os quais podem ser tratados sem exigências legais específicas, bem como menção expressa no artigo 5º, inciso I, de que dados anônimos não são considerados dados pessoais, como mencionado anteriormente.

Além disso, a redação do artigo pode ser aperfeiçoada, de modo a fazer menção apenas à possibilidade de identificação por parte do responsável pelo tratamento, excluindo-se o complemento "nem por qualquer outra pessoa". Isso porque o responsável desconhece que outros meios podem ser empregados por terceiros ("outras pessoas") em tentativas de reidentificação de dados anônimos.

Sugere-se, assim, que o conceito de dados anônimos previsto no artigo 5º, inciso IV do APL seja alterado para "*dados sobre um titular que não possa ser identificado pelo responsável pelo tratamento, tendo em conta o conjunto de meios suscetíveis de serem razoavelmente utilizados para identificar o referido titular*".

e) Aperfeiçoamento sobre consentimento

O texto atual do APL dispõe em seu artigo 5º, inciso VII, que consentimento é a *"manifestação livre, expressa, específica e informada pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada"*, ao passo que o artigo 7º do APL estabelece, como regra geral, que dados pessoais somente podem ser objeto de tratamento *"após o consentimento livre, expresso, específico e informado do titular"*.

O anteprojeto de Lei distancia-se do direito europeu ao adotar o conceito de "consentimento expresso" como regra geral. O art. 7º da Diretiva Europeia 95/46/CE menciona apenas "consentimento" de forma genérica, o que tem sido entendido na Europa como equivalente ao consentimento inequívoco, que pode ser obtido tanto de modo expresso quando inferido pelas circunstâncias e pelo contexto do tratamento dos dados.

O direito europeu reserva o consentimento expresso como regra geral apenas para as hipóteses de tratamento de dados considerados sensíveis, como se observa do art. 8º da Diretiva Europeia 95/46/CE.

A adoção de um conceito de consentimento *inequívoco*, em oposição a expresso, viabiliza o tratamento de dados no ambiente online, permite a contínua inovação baseada em dados e assegura um nível de proteção adequado ao titular sem gerar ônus excessivos para os responsáveis pelo tratamento de dados.

Ademais, do ponto de vista do titular dos dados, a exigência de obtenção de consentimento expresso para toda e qualquer atividade de tratamento de dados gera um fenômeno conhecido como "fadiga de consentimento", em que o titular passa a concordar com todo e qualquer pedido de consentimento, ficando paradoxalmente menos protegido por não prestar atenção às hipóteses de tratamento que envolvem riscos maiores e que mereceriam maior cautela por parte do titular.

Sugere-se, portanto, a alteração do conceito de consentimento no anteprojeto de Lei, tanto no art. 5º, quanto no art. 7º, para que seja mencionado que consentimento é a manifestação "livre, inequívoca e informada do titular", bem como que dados pessoais somente podem ser objeto de tratamento "após o consentimento livre, inequívoco e informado do titular".

f) Exceção ao consentimento: o interesse legítimo

O texto atual do anteprojeto de Lei dispõe em seu artigo 7º que, como regra geral, dados pessoais somente podem ser objeto de tratamento "após o consentimento livre, expresso, específico e informado do titular". Algumas exceções a essa regra geral são previstas no art. 11[1].

Na Diretiva Europeia, o consentimento do titular é apenas uma das modalidades que autorizam o tratamento de dados pessoais, não tendo o mesmo caráter de regra geral ora proposta, como se observa do artigo 7º da Diretiva Europeia 95/46/CE.

1 As exceções à necessidade de consentimento atualmente previstas no anteprojeto de Lei são: a) dados de acesso público irrestrito; b) quando o tratamento for indispensável para: I – cumprimento de uma obrigação legal pelo responsável; II – tratamento e uso compartilhado de dados relativos ao exercício de direitos ou deveres previstos em leis ou regulamentos pela administração pública; III – execução de procedimentos pré-contratuais ou obrigações relacionados a um contrato do qual é parte o titular, observado o disposto no § 1º do art. 6º; IV – realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a dissociação dos dados pessoais; V – exercício regular de direitos em processo judicial ou administrativo; VI – proteção da vida ou da incolumidade física do titular ou de terceiro; VII – tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias.

Uma das principais modalidades de tratamento de dados pessoais no sistema europeu é a existência de um interesse legítimo por parte do responsável. De acordo com essa modalidade, dados podem ser regularmente tratados, sem a necessidade de obtenção de consentimento, sempre que o responsável tiver interesse legítimo em tal tratamento, fazendo um balanceamento com os interesses, direitos e liberdades fundamentais do titular dos dados.

Ao interpretar esse dispositivo da Diretiva Europeia, o grupo de autoridades de proteção de dados da Europa, conhecido como "*Article 29 Working Party*", afirmou que essa modalidade de tratamento de dados estipula que o responsável faça um balanceamento ("*balancing test*"), entre seus interesses legítimos no tratamento dos dados e os interesses e direitos fundamentais do titular dos dados. O resultado desse balanceamento determina se os dados podem ou não serem legalmente tratados sem o consentimento do titular.

O *Article 29 Working Party* ressalta que esse balanceamento assegura aos responsáveis a flexibilidade necessária para efetuar o tratamento de dados nos casos em que não haveria impactos indevidos sobre o indivíduo em decorrência desse tratamento de dados. Por exemplo, o *Article 29 Working Party* considera que algumas atividades de marketing seriam permitidas, considerando esse balanceamento.

A importância do interesse legítimo fica ainda mais evidenciada quando se constata que o conceito tradicional de consentimento não é adequado para lidar com o tratamento de dados em larga escala ("*big data*") nem com o cenário de novos dispositivos conectados (Internet das coisas). A inclusão da hipótese de interesse legítimo no anteprojeto de Lei brasileiro traria a segurança jurídica necessária para que o tratamento de dados pudesse ser efetuado de modo seguro e lícito pelos responsáveis, sem onerar os titulares com a necessidade de manifestação de seu consentimento a cada instante.

Nesse contexto, sugere-se a introdução, entre as exceções ao consentimento previstas no art. 11 do anteprojeto de Lei, do interesse legítimo do responsável como hipótese expressa de autorização para tratamento de dados pessoais, por meio da inclusão de um inciso adicional, com a seguinte redação:

VIII – a persecução de interesses legítimos do responsável, desde que o tratamento seja feito de acordo com os princípios desta Lei e sejam preservados os direitos e garantias do titular.

Adicionalmente, o legislador pode optar por incluir alguns parâmetros para a hipótese de tratamento de dados em razão de legítimo interesse do responsável, desde que se atente para estes elementos:

(i) esse parâmetro não pode ser rígido para que não atrapalhe a inovação, pois o legítimo interesse pode mudar com o tempo e o avanço da tecnologia;

(ii) o legítimo interesse não pode infringir direitos fundamentais do usuário; e

(iii) é importante considerar, ainda, (a) a natureza do legítimo interesse; (b) o impacto de tal uso no titular; (c) a relação entre responsável e titular; e (d) questões de segurança.

Note-se que o responsável deve ser capaz de efetuar o tratamento com base no legítimo interesse sem obrigações adicionais. Afigura-se desnecessário, portanto, informar continuamente o titular a cada vez que o processamento ocorrer com base no legítimo interesse, pois o nível de transparência exigido depende do relacionamento entre responsável e titular (pode ser realizado, por exemplo, por meio de políticas de privacidade, configurações de privacidade, notificações sobre anúncios etc.)

Além disso, o tratamento realizado com base no legítimo interesse não deve exigir documentações adicionais ou inversões de ônus probatórios. Afigura-se muito mais importante promover a transparência do tratamento por meio de controles e outras salvaguardas do que exigir a documentação de cada hipótese de tratamento ocorrida com base no legítimo interesse.

3) Conclusão

Agradecemos pela oportunidade de apresentar nossas contribuições, esperando estimular o aprofundamento das reflexões em torno da regulamentação da proteção de dados pessoais no Brasil, permanecendo à inteira disposição deste Ministério da Justiça para colaborar em tudo que esteja ao seu alcance, visando à plena realização de todos os objetivos que orientam o uso da Internet no Brasil.

Atenciosamente,

Guilherme Ribenboim
Presidente do IAB Brasil

Marcel Leonardi
Presidente do Comitê de Assuntos Jurídicos – IAB Brasil