1 de julho de 2015

Excelentíssimo Senhor Ministro José Eduardo Cardozo
Ministro de Estado da Justiça
Ministério da Justiça
Esplanada dos Ministérios. Bloco T
5º andar, sala 538
Brasília, DF CEP 70064-900

Ref.: Consulta Pública sobre o Anteprojeto de Lei para a Proteção de Dados Pessoais

Excelentíssimo Senhor Ministro,

I – INTRODUÇÃO:

A BSA| The Software Alliance[1] agradece a oportunidade de participar da importante discussão sobre o futuro da proteção de dados no Brasil através da apresentação dos comentários abaixo referentes ao Anteprojeto de Lei para a Proteção de Dados Pessoais (doravante "Anteprojeto") publicado pelo Ministério da Justiça em 28 de janeiro de 2015.

Os membros da BSA têm um comprometimento profundo e duradouro com a proteção de dados de consumidores em diferentes tecnologias e modelos de negócios pois reconhecem que os consumidores só se sentem confortáveis em aproveitar os benefícios de novas tecnologias quando sabem que não perderão o controle sobre seus dados pessoais.

[1] *BSA | The Software Alliance (www.bsa.org) é a principal representante do setor de software global perante governos e no mercado internacional. Seus membros incluem as empresas mais inovadores do mundo, criando soluções de software que aquecem a economia e melhoram a vida moderna. Sediada em Washington, DC, e com operações em mais de 60 países ao redor do mundo, a BSA é pioneira em programas de conformidade que promovem o uso de software legítimo e promove políticas públicas que fomentam a inovação em tecnologia e fortalecem o crescimento da economia digital.*
Entre os membros da BSA estão: Adobe, Altium, Apple, ANSYS, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, Dell, IBM, Intuit, Microsoft, Minitab, Oracle, PTC, salesforce.com, Siemens PLM Software, Symantec, Tekla, The MathWorks, e Trend Micro.

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org

Assim, a BSA parabeniza e apoia os esforços do governo brasileiro em oferecer uma estrutura jurídica abrangente para a proteção de dados pessoais e recomenda fortemente que o Brasil continue trabalhando para promover um regime regulatório balanceado que proteja a privacidade dos consumidores sem comprometer a inovação e o potential da economia digital.

Como uma organização global, a BSA acompanha ativamente o desenvolvimento da legislação na área de privacidade de dados em todo o mundo, incluindo a União Europeia (UE). Observamos que o Anteprojeto abarca muitos dos objetivos e princípios louváveis da atual estrutura jurídica de proteção de dados da UE, bem como alguns dos conceitos que surgiram durante o processo de reforma da mesma atualmente em curso.

Embora a estrutura europeia baseada na Diretiva de Proteção de Dados (95/46/EC) ofereça um arcabouço de proteção de dados pessoais, alguns de seus princípios têm sido debatidos amplamente, pois eles podem não estar aptos para suprir a evolução das necessidades dos usuários quando tecnologias e serviços inovadores estão criando novas maneiras de se comunicar, socializar e fazer negócios.

Como vários aspectos do Anteprojeto brasileiro têm base na experiência europeia, alguns de nossos comentários incluirão reflexões sobre a estrutura europeia atual e a proposta de revisão da mesma já que tais considerações podem ser úteis para o Brasil na criação de sua própria legislação de proteção de dados.

Nossas considerações a respeito dos seguintes tópicos podem ser encontradas nas próximas páginas:

- Escopo Territorial
- Definição de Dados Pessoais
- Consentimento
- Outras Bases Legítimas para o Tratamento
- Alocação de Responsabilidade e Obrigação
- Transferências Internacionais de Dados
- Violação de Dados

II - COMENTÁRIOS SOBRE DISPOSIÇÕES ESPECÍFICAS DO ANTEPROJETO:

Escopo Territorial – Artigo 2[2]

O uso difundido da Internet, os serviços baseados na nuvem, o crescimento da "Internet das Coisas" e a contínua expansão da economia movida por dados faz com que a aplicação do princípio da territorialidade fique mais complexa, já que pode ser praticamente impossível identificar a localização exata de uma atividade que acontece online e determinar que a mesma tenha ocorrido em um determinado país.

Portanto, nos preocupamos com o conceito de que o escopo da lei seja definido em função do local da "operação de tratamento". Em nossa opinião, haveria mais segurança jurídica caso o escopo territorial determinado pela lei fosse modificado de forma que a jurisdição brasileira seja estabelecida quando um produto ou serviço for "especificamente direcionado" a consumidores ou usuários que residam no Brasil no momento da coleta e que a coleta seja feita por entidade que tenha conexão com o Brasil. Essa abordagem é utilizada por leis internacionais relacionadas a serviços online[3].

Assim, recomendamos que a redação do Artigo 2 seja modificada da seguinte forma:

Art. 2º *Esta Lei aplica-se a qualquer operação de tratamento realizada por meio total ou parcialmente automatizado, por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do país de sua sede e do país onde esteja localizado o banco de dados, desde que a informação coletada seja referente a cidadão brasileiro ou pessoa residente no Brasil e a coleta da informação seja feita por entidade estabelcida no Brasil ou sujeta a leis brasileiras em virtude de regras de direito internacional.*

§ 1º *Esta Lei não se aplica aos tratamentos de dados:*

I *– realizados por pessoa natural para fins exclusivamente pessoais; ou*
II *– realizados para fins exclusivamente jornalísticos.*

§ 2º *É vedado aos órgãos públicos e entidades públicas efetuar a transferência de dados pessoais constantes de bases de dados que administram ou a que tenham acesso no exercício de suas competências legais para entidades privadas, exceto em*

[2] O número dos artigos mencionados neste documento são referentes ao Anteprojeto de Lei para a Proteção de Dados Pessoais divulgado pelo Ministério da Justiça em 28 de janeiro de 2015.

[3] Por exemplo, a Diretiva para Proteção de Dados Pessoais da UE utiliza abordagem semelhante em seu Artigo 4

casos de execução terceirizada ou mediante concessão e permissão de atividade pública que o exija e exclusivamente para fim específico e determinado.

Definição de Dados Pessoais – Artigo 5

Observamos que a definição tem base no conceito de dados pessoais utilizado na regulamentação de proteção de dados da Europa, que inclui qualquer tipo de informação, independentemente de forma ou conteúdo, esteja tal informação ligada a uma pessoa física identificada ou identificável ou não.

No entanto, essa definição ampla está sendo discutida na Europa e já teve impacto na região – por exemplo, algumas pesquisas na UE na área da medicina não foram conduzidas conforme planos originais devido a exigências rigorosas de autorização prévia mesmo que os titulares não pudessem ser identificados diretamente pelo controlador de dados. É provável que a aplicação de obrigações jurídicas muito rigorosas aplicada a uma vasta gama de dados, independentemente do contexto e potencial de danos ao usuário, reduza a inovação orientada por dados no Brasil, com impacto negativo sobre o crescimento econômico.

Por isso, sugerimos que a legislação brasileira adote um conceito de dados pessoais baseado no contexto, sob o qual os dados sejam considerados "dados pessoais" somente quando a pessoa responsável relevante possa identificar o indivíduo a quem os dados pertencem. O contexto e circunstâncias particulares de um caso específico têm impacto direto sobre a possibilidade de identificação, por isso a abordagem contextualizada, conforme explicado pelo Parecer 05/2014 do *European Advisory Board Working Party 29*.

Isso é ainda mais importante porque o escopo do regime de proteção de dados proposto no Brasil parece ser mais amplo do que o que ocorre atualmente na Europa, explicitamente incluindo no artigo 5 (I) dados que não sejam necessariamente pessoais, tais como dados de localização ou identificadores eletrônicos.

Dados de localização que não estejam ligados a uma pessoa identificável (tais como o nome de uma rede sem fio local) levantam menos questões de privacidade e não merecem ser regulamentados como dados pessoais. Considerar tais dados como "pessoais" serviria apenas para criar obstáculos à prestação de serviços de localização geográfica demandada por consumidores sem aumentar sua privacidade.

Adicionalmente, as leis europeias também reconhecem que identificadores online (ou eletrônicos) tais como endereços de protocolo de internet (*IP protocol addresses)* ou *cookies* não precisam ser necessariamente considerados dados pessoais em todos os casos. Sujerimos, assim, que o Brasil siga esta abordagem prudente.

Logo, recomendamos a exclusão da referência explícita a esses dados do Artigo 5 (I).

Art. 5º Para os fins desta Lei, considera-se:

I – dado pessoal: dado relacionado à pessoa natural identificada ou identificável;

Consentimento – Artigos 7 e 10

Apesar de reconhecermos que o consentimento do titular pode ser uma forma válida de legitimar o tratamento de dados pessoais, nossa preocupação é que – ao contrário da prática em outros países – isso seja apresentado pelo anteprojeto brasileiro como o principal meio de legitimação do processamento. Isto é problemático, pois em muitos casos pode não ser adequado ou apropriado para o agente ou a pessoa responsável obter autorização para a legitimação de coleta e processamento de dados.

Por exemplo, se uma instituição financeira coleta informações sobre uma dívida pendente para autorizar os procedimentos de cobrança, pode não ser adequado solicitar a autorização do titular para fazê-lo, mas existe um interesse comercial legítimo que justificaria a coleta, ou seja, a cobrança (vide a próxima seção para maiores detalhes sobre interesse comercial legítimo).

Os controladores de dados devem ser responsáveis pela segurança dos dados confiados a eles. Como pode ser difícil oferecer e/ou obter consentimento, dependendo das circunstâncias, e as organizações passem a usar o interesse legítimo ou outra base jurídica para o processamento, o modelo de responsabilidade estabelecido pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE) pode ser utilizado para garantir que as empresas tenham disponíveis as ferramentas, políticas e programas que garantam a elas a tomada de decisões responsáveis sobre a proteção e uso de dados. Salientamos que o modelo da OCDE foi endossado e integrado em diversos sistemas jurídicos e princípios de privacidade, incluindo as Regras de Privacidade Internacionais (CBPR) da APEC e a Lei de Proteção de Informações Pessoais do Canadá.

Apesar das exceções descritas no Artigo 11, acreditamos que o consentimento não deve ser apresentado como exigência principal e todas as bases legais para o processamento devem ser vistas como igualmente válidas.

Em casos onde o consentimento seja necessário, é importante que a legislação foque nos fins, e não nos meios, de se obter tal autorização.

Logo, acreditamos que a lei brasileira deva reconhecer a validade de uma variedade de mecanismos para obtenção de consentimento, incluindo um recurso de *opt-out* informado e de fácil acesso.

Permitir vários mecanismos para consentimento é ainda mais importante considerando o advento da "Internet das Coisas" e os dados resultantes que podem ser analisados e utilizados para criar benefícios sociais e econômicos.

No mundo de hoje, uma grande quantidade de informações é criada através das interações com aparelhos conectados à internet e o consentimento expresso não é apropriado em todas os casos. Por exemplo, se um indivíduo tivesse que conceder autorização expressa para permitir que os dados gerados por ele toda vez que ele tocasse o seu cartão magnético de transporte público em um leitor eletrônico por ocasião de sua entrada em um sistema de transporte público, pesquisas para melhorar os serviços de transporte baseadas na análise dos dados gerados por tal prática, em conjunto com dados gerados por outros usuários do sistema público de transportes, poderia ser amplamente dificultada ou até mesmo impossibilitada. Se o Brasil apenas depender de consentimento expresso como base para o processamento de informações, há o risco de que o país não possa se beneficiar das melhorias geradas pela economia baseada em dados.

Solicitar consentimento expresso de forma excessiva pode gerar "fatiga" e os usuários podem passar a aceitar quaisquer termos apresentados a eles apenas para conseguirem acessar rapidamente o serviço que buscam. De fato, existe uma grande variedade de mecanismos que permitem aos usuários controlar e autorizar a coleta e uso de suas informações, e alguns dos mecanismos de *opt-out* robustos oferecem maior proteção da privacidade ao consumidor (com menos ônus aos usuários da Internet) do que mecanismos mais fracos de *opt-in*.

Cabe observar que tal prática estaria alinhada às atuais leis de proteção de dados da UE, que definem consentimento como qualquer "indicação específica e informada de livre e espontânea vontade". Na interpretação das autoridades de proteção de dados, não deve haver ambiguidade, mas isso não significa que o *opt-in* é a única alternativa: um modelo de *opt-out* pode incluir todas as 4 condições exigidas (indicação de livre e espontânea vontade, específica, informada e sem ambiguidade).

Observe-se também que a lei europeia aplica uma abordagem de dois níveis ao consentimento, reservando a exigência de consentimento "explícito" (ou expresso nos termos do Anteprojeto brasilieiro) somente aos casos em que os dados processados sejam de natureza altamente sensível.

Portanto, acreditamos que a referência ao consentimento "expresso" como única base para o processamento deva ser removida do Anteprojeto de forma geral. Por

exemplo, o texto do *Artigo 2, VII,* deveria suprimir o uso do termo expresso e deveria ter a seguinte redação:

VII – consentimento: manifestação livre, específica e informada pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

Por último, observamos que, em situações onde o consentimento pode ser exigido, ele só deve ser obtido pela segunda vez caso haja alterações relevantes. Portanto, sugerimos que a palavra "relevantes" seja adicionada ao artigo 10, § 2, cuja redação passaria a ser:

§ 2 Em caso de alterações relevantes de informação referida nos incisos I, II, III, ou V do caput, o responsável deverá obter novo consentimento do titular, após destacar de forma específica o teor da alteração.

Outras Bases Legítimas para o Tratamento – Artigo 11

Nos termos da estrutura jurídica europeia, as três bases mais importantes para a coleta de dados por agentes comerciais que não trabalhem diretamente no setor público são: contrato, consentimento e o interesse legítimo. Lamentamos que esta última base não conste do Anteprojeto brasileiro.

De fato, a base jurídica representada pelo interesse legítimo do agente tem um papel importante pois pode não ser apropriado para o proprietário ou a pessoa responsável obter autorização para legitimar a coleta ou tratamento de dados ou pode ser prematuro celebrar um contrato com um consumidor.

O interesse comercial legítimo como base para o processamento se tornou ainda mais importante com o advento da análise de *Big Data* e da Internet das Coisas. Considerar o interesse legítimo como base adequada para o tratamento permitirá o surgimento de novos negócios baseados na análise de dados no Brasil.

O interesse legítimo também pode representar vantagem direta sob a perspectiva de proteção e minimização de dados. Isso se deve ao fato de que contrato e autorização exigem ou incentivam, direta ou indiretamente, a identificação do proprietário. Por outro lado, a base jurídica do interesse legítimo não exige ou incentiva tal identificação. Assim, sua disponibilidade e uso é consistente, e encoraja, a minimização de dados.

Apesar da Diretiva para Proteção de Dados da EU não definir o termo "interesse legítimo", diretrizes detalhadas para o uso do critério foram estabelecidas pela WP

29[4]. O uso desta base jurídica está condicionada a um teste de equilíbrio cuidadosamente elaborado que serve o propósito de facilitar o tratamento de dados ao mesmo tempo em que protege os direitos dos usuários. Deste modo, a utilização da base jurídica representada pelo interesse legítimo está sujeita a dois teste. O primeiro é a legitimidade do interesse do agente. O segundo é a comparação desse interesse aos direitos fundamentais do titular. Caso o segundo tenha mais peso do que o primeiro, o interesse legítimo não pode ser utilizado como base para o processamento. A base jurídica do interesse legítimo também é combinada com o direito de objeção do titular dos dados. O resultado desse teste de equilíbrio irá determinar se o interesse comercial legítimo pode ser utilizado como base para o processamento.

O WP 29 emitiu uma parecer específico sobre essa questão, e declarou que "O WP29 reconhece a significância e utilidade do critério do Artigo 7(f), que nas circunstâncias corretas, e com as resguardas adequadas, pode ajudar a prevenir o respaldo demasiado em outras bases jurídicas. O Artigo 7(f) não deve ser tratado como 'último recurso' em situações raras ou inesperadas em que outras bases para o processamento legítimo não se apliquem. Entretanto, ele não deve ser a escolha automática, e seu uso não deve ser estendido sob a percepção de que é menos restritivo do que outras bases".

Em suma, considerando os benefícios à privacidade inerentes a essa interpretação e as sólidas cautelas que a permeiam, acreditamos que:

- conforme delineado no Artigo 7(f) da atual Diretriz de Proteção de Dados Europeia (Artigo 6(f) em certos casos), o interesse legítimo evitaria um ônus muito grande sobre o titular para entender todos os usos potenciais de suas informações em uma arena de fluxo de dados cada vez mais complexa. Conforme mencionado acima, o advento de *Big Data* e da Internet das Coisas torna o interesse legítimo ainda mais relevante como base para o tratamento;
- a introdução da base jurídica do interesse legítimo traria benefícios significativos aos agentes e titulares de dados brasileiros.

Assim, recomendamos a inclusão de uma nova cláusula VIII no Artigo 11, a saber:

VIII –para a realização de objetivos de interesse legítimo do agente, exceto quando tais interesses sejam sobrepostos pelos direitos fundamentais descritos no Artigo 1.

Além disso, observamos que na UE, o tratamento de dados necessários para garantir segurança de rede e da informação constitui uma operação de processamento legítima. Isso é importante para que as empresas possam proteger sua rede e os

[4] Diretriz do WP 29 sobre o uso do controlador dos dados com base no artigo 7 da Diretiva 95/46/EC pode ser encontrada no link http://www.cnpd.public.lu/fr/publications/groupe-art29/wp217_en.pdf

dados pessoais confiados a elas por meio da prevenção ao acesso não-autorizado, distribuição maliciosa de código, ataques de serviço, etc.

Assim, sugerimos ao governo brasileiro a inclusão da seguinte cláusula no Artigo 11:

"IX – garantir a segurança da rede e da informação e prevenir fraudes."

Alocação de Responsabilidade e Obrigação– Artigos 11, 22, 31, 37 e 39

Destacamos que o propósito da distinção entre a pessoa responsável e o agente (ou o controlador e o processador, conforme referidos na lei europeia) é oferecer clareza de responsabilidade perante o titular dos dados, bem como para o cumprimento das exigências legais. Segundo a legislação atual da UE, toda responsabilidade recai sobre a pessoa responsável.

O operador, conforme descrito no Artigo 39 do anteprojeto de lei, age "em nome" da pessoa responsável, ou seja, o tratamento conduzido por essa entidade é determinado pelo mandato outorgado pela pessoa responsável ao operador, e portanto, em geral, regido por contrato.

Essa clara alocação de responsabilidade e obrigação jurídica é crucial e garante que a prática crescente e difundida da terceirização não cause confusão no sistema: o titular dos dados e as autoridades sabem a quem recorrer caso ocorra um problema, e as empresas têm clareza sobre funções e responsabilidades.

A atribuição de responsabilidade direta, conjunta e acentuada sobre o operador / outorgado, conforme estabelecido pelo anteprojeto de lei (artigo 11, § 3; artigo 22; artigo 31, artigo 37; artigo 39, § 1), resultaria em várias consequências imprevistas e abalaria o relacionamento entre esses agentes, criando um encargo de cumprimento injustificado e acabaria contrariando o princípio de privacidade da minimização de dados.

Assim, recomendamos fortemente que a lei brasileira siga os conceitos bem-estabelecidos e funcionais do regime europeu, onde a obrigação e responsabilidade perante o titular dos dados são atribuídas à pessoa responsável ou outorgante. Recomendamos, assim, a exclusão das referências à responsabilidade do outorgado e/ou operador nos artigos 11, § 3; artigo 22; artigo 31, artigo 37; artigo 39, § 1.

As relações entre o operador e a pessoa responsável, bem como entre o outorgante e outorgado, devem ser regidas por contratos ou outros atos legalmente vinculantes, cuja violação sujeitaria as partes às disposições do Código Civil.

As pessoas responsáveis (controladoras) devem ter a obrigação de garantir o cumprimento da lei de privacidade de dados aplicável, enquanto os operadores (processadores) devem seguir as instruções dadas pelas pessoas responsáveis e garantir a segurança dos dados que eles processam. Estas são responsabilidades usualmente conferidas às pessoas responsáveis e aos operadores em leis de privacidade no contexto internacional. Recomendamos, assim, que o Brasil siga tais parâmetros.

Direitos do Titular – Artigos 17 e 18

Existem circunstâncias em que não é possível fornecer a um titular informações sobre seus próprios dados sem a divulgação de informações que pertençam a outros titulares (por exemplo, quando as informações fazem parte de arquivos ou bases de dados que não podem ser modificados para segregar informações de um indivíduo). Isso deve ser levado em conta ao se estabelecer o direito de acesso de dados de uma determinado titular e, portanto, recomendamos que o artigo 17, II seja alterado de forma a incluir tal exceção. Assim, sugerimos a seguinte redação:

II – Acesso aos dados, a menos que tal acesso não seja viável sem a revelação de informações pertencentes a outros titulares de dados.

Além disso, a legislação proposta determina que as informações devem ser fornecidas sem custo para o titular mediante solicitação. Isso pode causar um ônus excessivo, especialmente para pequenas e médias empresas. Logo, sugerimos que o artigo 17, § 4 seja alterado de maneira a dispor que as informações serão fornecidas sem custo excessivo ao titular dos dados. Assim, sugerimos a seguinte redação:

§ 4º - A providência de que trata o § 2º será realizada sem custo excessivo para o titular.

Com relação ao prazo máximo para o fornecimento das informações, o período de sete dias determinado no artigo 17, § 3 é extremamente curto. Recomendamos alterar o texto de forma a declarar que as informações devem ser fornecidas sem demora excessiva. Assim, sugerimos a seguinte redação:

§ 3º Em caso de impossibilidade de adoção imediata da providência de que trata o §2º, o responsável enviará ao titular, sem demora excessiva, resposta em que poderá:
I – comunicar que não é agente de tratamento dos dados; ou
II – indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

Finalmente, o artigo 18 confere ao titular dos dados a capacidade de escolher entre receber as informações solicitadas de forma eletrônica ou em cópia física ("formato impresso"). Para que o processador dos dados forneça as informações solicitadas de maneira eficiente e sem ônus excessivo, o artigo 18 deveria ser alterado para determinar que o formato eletrônico deve ser o formato padrão. O fornecimento em qualquer outro formato, incluindo cópia física, deve ser uma exceção apenas caso o titular dos dados declare a impossibilidade de acessar as informações por via eletrônica.

Assim, sugerimos a seguinte redação para o Artigo 18:

Art. 18. A confirmação de existência ou o acesso a dados pessoais serão providenciados, a critério do titular:
I – em formato simplificado, sem demora excessiva; ou
II – por meio de declaração clara e completa, que indique a origem dos dados, data de registro, critérios utilizados e finalidade do tratamento, fornecida sem demora excessiva.

§ 1º Os dados pessoais serão armazenados em formato que permita o exercício do direito de acesso.

§ 2º As informações e dados serão fornecidos, por meio eletrônico, seguro e idôneo.
I – Em casos excepcionais, a informação poderá ser fornecida de forma impressa, somente se o titular dos dados declarar a impossibilidade de acesso à informação por meio eletrônico. Nestes casos, poderá ser cobrado exclusivamente o valor necessário ao ressarcimento do custo dos serviços e dos materiais utilizados.

§ 3º O titular poderá solicitar cópia eletrônica integral dos seus dados pessoais em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento, sempre que o banco de dados estiver em suporte eletrônico.

§ 4º Órgão competente poderá dispor sobre os formatos em que serão fornecidas as informações e os dados ao titular.

Transferências Internacional de Dados – Artigo 28

A abordagem "transferência proibida a menos que..." da legislação europeia tem sido bastante criticada porque conflita com o vasto aumento de fluxo de dados globais que ocorreu nos últimos 20 anos, desde sua adoção.

Adicionalmente, os métodos dispostos pela lei europeia para a transferência de dados, tais como adequação, cláusulas de modelo e Regras Corporativas Vinculantes ("Biding Corporate Rules" ou BCRs) exigem que as empresas

enfrentem um processo longo e oneroso, tornando esses instrumentos inacessíveis para a maioria delas.

Em um mundo onde o fluxo internacional de dados deve ser a regra e não a exceção, as exigências legais devem ser projetadas de modo que seu cumprimento esteja ao alcance razoável de toda entidade que lide com informações pessoais.

Portanto, argumentamos que o primeiro modelo de responsabilidade estabelecido pela OCDE e subsequentemente endossado a integrado em diversos sistemas jurídicos e princípios de privacidade, incluindo as Regras de Privacidade Internacionais da Cooperação Econômica Ásia-Pacífico ("APEC's CBPR") e a Lei de Proteção de Informações Pessoais do Canadá - que recebeu uma determinação de adequação da UE - ofereceria uma abordagem à governança internacional de dados que conferiria ao indivíduo proteções e fomentaria fluxos robustos e otimizados de dados. Um modelo baseado na responsabilidade do agente exige que as organizações que coletam e utilizam dados sejam responsáveis por sua proteção e uso responsável, independentemente de onde e por quem sejam processados, e exige ainda que as organizações que transfiram dados tomem medidas adequadas para assegurar que todas as obrigações – estabelecidas em lei, diretrizes ou compromissos firmados em políticas de privacidade das organizações – sejam cumpridas.

Assim, recomendamos fortemente que o governo brasileiro considere as vantagens e desvantagens de todas as opções disponíveis antes de decidir a abordagem final no que tange a transferência internacional de dados.

Caso o modelo europeu seja escolhido, deve-se levar em conta exceções adicionais que estão sendo introduzidas como parte da contínua reforma legislativa, visando tornar o sistema um pouco mais flexível. Por exemplo, o reconhecimento de cláusulas padrão em contratos entre processadores está sendo considerado e seria um passo positivo rumo a uma maior flexibilidade do sistema. Outro exemplo seria o aumento da flexibilidade em transferências entre um grupo empresarial ou grupo de empresas que desenvolve uma atividade econômica em conjunto – a nova proposta considera permitir o uso de regras corporativas aprovadas para as transferências internacionais desses grupos da União Europeia para organizações dentro do mesmo grupo, desde que tais regras corporativas incluam princípios essenciais e direitos exequíveis para garantir a proteção apropriada em transferências ou categorias de transferências de dados pessoais.

Além disso, um sistema de reconhecimento mútuo para disposições contratuais padrão e padrões corporativos globais deve ser colocado em prática para evitar exigências globais múltiplas e potencialmente contraditórias. De fato, a WP 29 recentemente publicou diretrizes (*WP 226*) que irão oferecer maior segurança para empresas que transferem dados pessoais para fora da Europa.

Violação de Dados – Artigos 44 e 45

A BSA apoia a criação de um sistema de notificação de violação de dados aplicável a todos os negócios e organizações. Tal exigência poderia incentivar entidades a garantirem a proteção robusta de dados pessoais, ao mesmo tempo em que permitiriam aos titulares tomar medidas para sua própria proteção caso seus dados sejam comprometidos.

No entanto, qualquer proposta deve ser elaborada cuidadosamente para evitar a emissão de notificações irrelevantes, principalmente assegurando que se exija a notificação somente quando exista risco grave de dano ao usuário. Além disso, devem ser excluídos da obrigação de notificação todos os casos em que os dados comprometidos em questão tenham sido considerados inutilizáveis, ilegíveis ou indecifráveis por um terceiro não-autorizado devido ao use de práticas ou métodos amplamente aceitos como práticas ou padrões vigentes do setor.

Portanto, a redação do artigo 44 deveria ser alterada para exigir notificação em casos de incidentes “graves” de segurança, em vez de “quaisquer” incidentes.

Adicionalmente, a exigência de notificação “imediata” não é apenas excessiva, mas também prematura, pois as organizações precisam de tempo para determinar a existência da violação e realizar, no mínimo, uma verificação preliminar de seu impacto e possíveis consequências. Logo, em nossa perspectiva, o prazo para a exigência de notificação deve ser alinhado aos padrões internacionais atuais, e a legislação deve estabelecer que a notificação deve ser feita “sem demora indevida”. Sugerimos, assim, a seguinte redação para o Artigo 44:

Art. 44. O responsável deverá comunicar, sem demora indevida, ao órgão competente a ocorrência de incidentes de segurança sérios que possam acarretar prejuízo aos titulares.

Finalmente, embora uma divulgação pública conforme estabelecido pelo Artigo 45 (II) seja necessária em alguns casos, é crucial que ela seja feita somente após consulta prévia com a pessoa responsável ou operador. Isso é importante porque a divulgação pública pode causar mais danos ao proprietário dos dados, já que tornar pública a existência da vulnerabilidade pode levar a mais abusos em vez de contribuir para a solução do problema caso a divulgação não seja feita com cuidado. Logo, sugerimos que o artigo 45 (II) determine que a divulgação ampla seja feita somente após consulta prévia com a pessoa responsável.

Assim, sugerimos a seguinte redação para o Artigo 45:

Art. 45. Órgão competente poderá determinar a adoção de providências quanto a incidentes de segurança relacionados a dados pessoais, conforme sua gravidade, tais como:

I – pronta comunicação aos titulares;
II – ampla divulgação do fato em meios de comunicação <u>apenas depois de consulta abrangente com a pessoa responsável ou operador se tal divulgação não puder potencialmente acarretar danos adicionais ao titular dos dados</u>; ou
III – medidas para reverter ou mitigar os efeitos de prejuízo.

III – CONCLUSÃO:

Mais uma vez, gostaríamos de agradecer a oportunidade de participar deste diálogo que esperamos irá contribuir para a criação de políticas públicas que permitirão mais inovação e crescimento econônico gerado pela economia digital no Brasil.

Esperamos continuar participando desta importante discussão e colocamo-nos à disposição para esclarecer quaisquer dúvidas.

Atenciosamente,

Leticia S. Lewis
Diretora, Políticas Públicas
BSA|The Software Alliance

cc: Sra. Juliana Pereira da Silva, Secretária Nacional do Consumidor