08000.005377/2016-32

The Software Alliance

BSA

29 de fevereiro de 2016

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 a Minuta de Decreto que regulamentará a Lei nº 12.965, de 23 de abril de 2014

Excelentíssimo Senhor Ministro,

I – INTRODUÇÃO:

A BSA| The Software Alliance (BSA)[1] agradece a oportunidade de participar da consulta pública sobre a Minuta de Decreto que regulamentará a Lei nº 12.965, de 23 de abril de 2014 (doravante "Minuta do Decreto"). A referida consulta pública é extremamente relevante para a atual discussão sobre o futuro da proteção de dados no Brasil.

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

[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, ANSYS, Apple, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, DataStax, Dell, IBM, Intuit, Microsoft, Minitab, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, Tekla, The MathWorks, Trend Micro, and Workday.

20 F Street, NW, Suite 800
Washington, DC 20001

P 202-872-5500
W bsa.org

benefícios de novas tecnologias quando sabem que não perderão o controle sobre seus dados pessoais.

A BSA e nossos membros parabenizam o Ministério da Justiça por promover um amplo debate entre todos os interessados sobre as políticas públicas mais apropriadas para a proteção de dados no Brasil. Este debate está acontecendo através de discussões sobre a Lei para a Proteção de Dados Pessoais, cuja minuta foi elaborada pelo Ministério da Justiça e deve ser enviada ao Congresso Nacional em breve. Acreditamos que a melhor maneira de continuar avançando no debate sobre privacidade de dados é a utilização de tal canal.

A privacidade de dados é um tópico multidimensional que requer a consideração criteriosa de uma série de elementos para garantir que as políticas eventualmente adotadas sejam equilibradas no que tange à proteção de dados e à inovação. Também é importante que tais políticas permitam a continuação da expansão da economia digital. O debate sobre a Lei para a Proteção de Dados Pessoais é uma oportunidade de abordar a privacidade de dados de uma forma holística e efetiva. Apesar do Marco Civil da Internet e do Decreto que o regulamentará serem importantes, detalhes sobre privacidade de dados serão melhor abordados pela Lei para a Proteção de Dados Pessoais.

Alguns artigos da Minuta do Decreto podem inadvertidamente antecipar alguns aspectos da atual discussão sobre a Lei para a Proteção de Dados, o que pode criar obrigações contraditórias e/ou insegurança jurídica. Este fato gera preocupação.

A BSA e nossas empresas associadas parabenizam e apoiam os esforços do Brasil para a criação de uma política para a proteção de dados pessoais. Sugerimos que o governo brasileiro continue trabalhando através de um processo único para criar um regime legal para a proteção de privacidade de dados que vise proteger os usuários sem prejudicar a inovação e o poder da economia digital. Os comentários abaixo são oferecidos para contribuir com este objetivo.

II – COMENTÁRIOS SOBRE ARTIGOS ESPECÍFICOS DA MINUTA DO DECRETO:

A – Definição de Dados Pessoais e de Tratamento de Dados Pessoais (Minuta do Decreto, Artigo 12)

Como mencionado anteriormente, alguns dos artigos da Minuta do Decreto, incluindo as definições de dados pessoais e tratamento de dados pessoais, podem antecipar indevidamente aspectos importantes da discussão que está atualmente acontecendo

no contexto dos debates sobre a futura Lei para a Proteção de Dados Pessoais. Isto pode criar obrigações contraditórias e insegurança jurídica. Além disso, as definições podem ser consideradas inconstitucionais pois o Decreto pode não ser a norma mais apropriada para definir "dados pessoais" e "tratamento de dados pessoais".

Solicitamos respeitosamente, assim, que o Artigo 12 da Minuta do Decreto que define os termos "dados pessoais" e "tratamento de dados pessoais" seja modificado para fazer referência a definições que serão apresentadas por legislação específica sobre privacidade de dados, ou seja, a Lei para a Proteção de Dados Pessoais. Tal mudança evitará incertezas causadas por potenciais conflitos entre a Lei e o Decreto.

B – Critérios para Segurança da Informação (Minuta de Decreto, Artigo 11)

O Artigo 11 da Minuta do Decreto estabelece que certos critérios devem ser atendidos para garantir a segurança da informação. Segurança da informação é um dos tópicos que está sendo discutido no contexto da futura Lei para a Proteção de Dados Pessoais. Quaisquer requisitos estabelecidos pela Minuta do Decreto sobre este assunto podem tornar-se desatualizados e/ou criar obrigações conflitantes em relação à futura Lei para a Proteção de Dados Pessoais.

Acreditamos que eventuais diretrizes sobre a segurança de informação a serem adotadas pela Lei para a Proteção de Dados Pessoais devem permitir que se demonstre alinhamento com os critérios mínimos de segurança através da referência a critérios voluntários reconhecidos globalmente que tenham sido desenvolvidos através de um processo "multi-stakeholder".

Além disso, critérios de segurança da informação devem adotar uma abordagem baseada em riscos ao invés de um foco em requerimentos muito detalhados. As diretrizes devem permitir que as pessoas responsáveis pela informação implementem as medidas de segurança que sejam mais apropriadas para mitigar os riscos específicos que elas enfrentam.

A regulamentação de questões ligadas à privacidade também deve permitir flexibilidade suficiente para acomodar desenvolvimentos tecnológicos. Regras muito detalhadas podem deixar de reconhecer tecnologias novas e em evolução, o que pode colocar em perigo a segurança e a privacidade da informação ao invés de aumentá-las, visto que as pessoas responsáveis pela informação poderiam não conseguir usar os mecanismos mais atualizados e eficientes devido ao limite imposto por regras extremamente detalhadas.

Finalmente, a regulamentação não deve proibir ou exigir a aquisição ou o emprego de produtos ou tecnologias específicas, incluindo hardware ou software. As pessoas responsáveis pela informação buscam proteger uma grande gama de alvos contra uma

grande variedade de riscos potenciais. Políticas que visam proteger dados devem permitir a implementação de medidas de segurança que sejam mais apropriadas para mitigar os riscos específicos enfrentados por cada entidade para aumentar a efetividade de tais medidas. Garantir a neutralidade tecnológica é primordial para que tal objetivo seja alcançado.

Recomendamos, portanto, que o artigo 11 seja modificado para fazer referência aos critérios de segurança a serem introduzidos em virtude da Lei para a Proteção de Dados. A BSA sugere que tais critérios sigam os princípios supra referidos.

C – Obrigação de Divulgar Padrões de Segurança (Minuta do Decreto, Artigo 14)

A Minuta do Decreto estabelece que os provedores de aplicação e provedores de conexão devem divulgar a qualquer parte interessada, preferencialmente através de seus sítios na internet, os padrões de segurança que adotam. Apesar de entendermos que a finalidade da regra é assegurar que os usuários estejam confortáveis com o nível de cuidado empregado para proteger os seus dados, se o equilíbrio correto não for atingido, a regra ao invés de melhorar a proteção de dados colocaria os mesmos em risco.

A atual redação do artigo 14 pode ser interpretada como obrigação de divulgar detalhes excessivos sobre as medidas de segurança utilizadas. A revelação de detalhes específicos sobre medidas de segurança empregadas forneceria informações que poderiam ser usadas por malfeitores para contornar tais medidas. Detalhes específicos não ajudariam os titulares dos dados a entender melhor como a suas informações são protegidas já que tais detalhes seriam muito técnicos para o entendimento da maioria das pessoas. A regra poderia, portanto, colocar em risco a informação que está tentando proteger sem melhorar a segurança ou a confiança do titular dos dados.

Recomendamos, portanto, que o Artigo 14 seja modificado para permitir que as pessoas responsáveis pela informação garantam a sua proteção de acordo com os termos de suas políticas de segurança. Isso garantiria aos titulares dos dados que suas informações são protegidas sem divulgar detalhes excessivos sobre os métodos utilizados para atingir tal objetivo.

D – Acesso Decorrente de Decisão Judicial ou Determinação Legal (Minuta do Decreto, Artigo 13)

A Minuta do Decreto determina que os registros de conexão e de acesso a aplicações de internet, bem como de dados pessoais e do conteúdo de comunicações privadas, deverão ser mantidos em formato que facilite o acesso decorrente de decisão judicial ou determinação legal.

A regra parece ser muito ampla já que não está claro o que significa um "formato que facilite o acesso". Dados devem ser mantidos de acordo com melhores práticas globais de forma a mitigar riscos à segurança da informação.

Os responsáveis pela informação devem desempenhar esforços razoáveis para cumprir com os termos de ordem judiciais de acordo com as suas circunstâncias específicas, mas eles não devem ser obrigados a modificar a forma através da qual eles mantêm as informações para "facilitar acesso". Desvios das melhores práticas globais que já tenham sido testadas e aprovadas por especialistas do setor podem enfraquecer a segurança da informação sem necessariamente aumentar a efetividade das atividades das autoridades competentes.

O Artigo 10 do Marco Civil da Internet (Lei 12.965/2014), que estabelece a obrigação de disponibilizar os dados com base em decisões judiciais, não requer a regulamentação da obrigação através de Decreto ou de outra norma. Portanto, solicitamos respeitosamente que o Artigo 13 seja removido da Minuta do Decreto.

E – Relatório sobre Requisição de Dados Cadastrais (Minuta do Decreto, Artigo 10)

O Artigo 10 da Minuta do Decreto estabelece que a autoridade máxima de cada órgão público federal deverá publicar relatórios anuais sobre a requisição de dados cadastrais e que tais documentos devem conter o número de pedidos realizados, lista dos provedores de conexão ou de acesso a aplicações que receberam os pedidos, e o número de pedidos deferidos e indeferidos pelos provedores.

Apesar de entendermos que o objetivo de tais relatórios é garantir a transparência, tais documentos devem apenas conter informações agregadas e não específicas sobre cada provedor. Especificar os números de pedidos feitos e/ou atendidos por cada provedor pode prejudicar investigações já que as informações podem ser usadas como pistas sobre táticas de investigação. É importante notar que relatórios desta natureza emitidos em outros países apenas incluem informações agregadas para proteger as investigações.

Além disso, relatórios emitidos segundo os requerimentos estabelecidos no Artigo 10 não apresentariam um cenário totalmente correto uma vez que os provedores podem deixar de atender pedidos por razões fora de seu controle, incluindo pedidos que não

atendam a requisitos legais devidamente ou em virtude da indisponibilidade das informações requisitadas.

Solicitamos, portanto, que o Artigo 10 seja modificado para que, se as autoridades tiverem que emitir relatórios, os mesmos apenas incluam informações agregadas, como o número total de pedidos realizados pelo órgão público federal, e não contenham informações específicas sobre pedidos relacionados a cada provedor.

F – Entrada em Vigor (Artigo 20):

Devido à complexidade das obrigações estabelecidas pela Minuta do Decreto, recomendamos que seja concedido um prazo de pelo menos um ano para permitir a adaptação às novas regras. Sugerimos, assim, a modificação do artigo 20 para refletir tal prazo.

III - CONCLUSÃO

Mais uma vez, gostaríamos de agradecer a oportunidade de participar deste diálogo que esperamos que irá contribuir para a criação de políticas públicas que permitirão mais inovação e crescimento econômico 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: Gabriel Sampaio, Secretário, Secretaria de Assuntos Legislativos do Ministério da Justiça