2 de julho de 2015

Ministério da Justiça
Secretaria de Assuntos Legislativos
Esplanada dos Ministérios,
Palácio da Justiça - Bloco T
70064-900, Brasília, DF, Brasil
debatedadospessoais@mj.gov.br

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

Prezados Senhores(as),

No âmbito dos trabalhos do Ministério da Justiça para a elaboração de uma lei sobre proteção de dados pessoais, a Entertainment Software Association (ESA) aproveita essa oportunidade para fornecer comentários ao anteprojeto de lei que foi disponibilizado para consulta pública em 28 de janeiro de 2015 (o "Anteprojeto").

A ESA é uma associação norte americana exclusivamente dedicada às necessidades relacionadas aos negócios e relações públicas de empresas que publicam jogos para computador, videogame, dispositivos móveis, notebooks e internet.

A ESA e seus membros tratam a proteção de dados com seriedade e os membros da ESA, na condição de empresas com operações globais, estão sujeitos às normas de proteção de dados por todo o mundo. Nesse sentido, nós gostaríamos de compartilhar nossa experiência em outras jurisdições e contribuir para a elaboração de uma legislação para a proteção de dados pessoais no Brasil que encoraje a inovação e o desenvolvimento dos negócios que operam na Internet, ao mesmo tempo em que fortaleça o direito à privacidade.

Nós também iremos submeter esses comentários por meio da plataforma online da consulta

pública.

1. Escopo Territorial (Artigo 2)

1.1. O critério estabelecido no artigo 2º é um desafio para serviços online, uma vez que nem sempre é possível ou simples determinar onde exatamente o titular dos dados se encontra no momento que os dados pessoais precisam ser coletados. Acreditamos que uma abordagem mais efetiva nesses casos seria determinar que a lei se aplica sempre que um serviço/produto online seja especificamente dirigido aos consumidores brasileiros e os responsáveis pelos dados coletem dados pessoais desses consumidores.

2. Definição de Dados Pessoais (Artigo 5, I)

2.1. A definição de dado pessoal deveria ser restringida para estabelecer que somente dados que permitam a identificação de um indivíduo sejam considerados dados pessoais. Nesse contexto, incluir dados locacionais ou identificadores eletrônicos na definição não é apropriado, uma vez que esse tipo de dado (endereços de IP, identificadores de cookies, etc.) não necessariamente permite a identificação de indivíduos, mas somente a identificação de computadores ou terminais. A adoção de um conceito mais abrangente de dado pessoal (como atualmente proposto) pode desincentivar a condução de negócios que requeiram algum nível de tratamento de dados pessoais no Brasil. Se restringir a definição não for viável, então recomendamos ao menos esclarecer que dados pessoais não incluem dados anônimos e não identificáveis. Essas mudanças ajudariam a encorajar o uso de dados anônimos.

3. Consentimento (Artigo 5, VII e Artigo 7)

3.1. Ao mesmo tempo em que é imprescindível que os indivíduos sejam informados sobre o tratamento de dados, estabelecer como regra que o consentimento deve ser expresso e específico pode ser problemático e não necessariamente assegura uma maior proteção aos direitos de privacidade dos indivíduos. Isso também pode se tornar um problema prático, conforme a tecnologia evolui e a disponibilidade de serviços e produtos online aumenta. A nosso ver, o consentimento não deveria ser considerado como a única base legal para o tratamento de dados, a ser dispensado somente nos casos listados no artigo 11 do anteprojeto.

3.2. Por exemplo, o consentimento deveria ser implícito para práticas usuais de coleta e uso de dados como: processamento de uma operação solicitada pelo consumidor, *first-party marketing*, monitoramento de serviços, autenticação, prevenção de fraudes, segurança de dados, pesquisa analítica ou sem caráter publicitário, transferência de dados a um terceiro para prestação de um serviço ao consumidor e outras atividades que suportem as operações internas do website ou serviço. Nesses casos, outras jurisdições tem acertadamente admitido que dados sejam tratados sem consentimento expresso quando existe um interesse legítimo do responsável. É esse o caso, por exemplo, quando dados precisam ser tratados para dar suporte, entregar e melhorar uma variedade de serviços em benefício do titular de dados. Para assegurar a sua confiabilidade, o tratamento de dados a serviço de um interesse comercial legítimo deve ser balanceado com a obrigação de proteger os direitos do titular dos dados de forma a não prejudicar tais direitos indevidamente. Isso se torna mais relevante na medida em que o tratamento de dados (data analytics) em larga escala e a internet das coisas se desenvolve, colocando o tratamento de dados em um ambiente mais complexo, em que o consentimento pode não ser a base mais apropriada ou efetiva para o tratamento de dados.

3.3. Quando o consentimento for exigido, é importante que a lei não crie obrigações excessivas para a sua obtenção ou privilegie a forma sobre o conteúdo. Além do consentimento escrito, há uma grande variedade de mecanismos que podem ser utilizados para obtenção de consentimento – e eles não necessariamente representam uma proteção menor da privacidade dos indivíduos em comparação com um consentimento expresso e escrito. Nesse sentido, deveria ser claro que o consentimento não precisa ser expressado por escrito apenas, conforme definido no artigo 7, § 3º, mas também pode ser fornecido eletronicamente, por meio de mecanismos de opt-in ou opt-out. Nesse sentido, salientamos que mecanismos de opt-out (em que o tratamento de dados é considerado autorizado a menos que o indivíduo expressamente se manifeste de forma contrária), somados a informações completas e de fácil entendimento sobre políticas de privacidade são com frequência uma maneira bastante efetiva de lidar com o consentimento em negócios online, sem reduzir a proteção oferecida aos dados pessoais e direito à privacidade. Tendo em vista o acima exposto, acreditamos que a referência a consentimento "expresso" deveria ser excluída.

3.4. Exigir que o consentimento seja "específico" também dificulta o fornecimento de

informações precisas e relevantes ao titular de dados e, conforme a tecnologia e aplicações de dados evoluem, pode se tornar impraticável – principalmente porque isso pode resultar em uma série de solicitações de consentimento, o que pode ser negligenciado pelo titular de dados. Requerer constantemente que indivíduos forneçam consentimento para todos os tipos de tratamento de dados pode de fato insensibilizá-los com relação à importância de assuntos relacionados à privacidade de dados. Em conjunto, essas exigências aumentam o nível de burocracia dos negócios e desfavorecem a inovação, especialmente considerando a velocidade das mudanças tecnológicas. Por essa razão, nós entendemos que a referência a consentimento "específico" também deveria ser excluída ou, ao menos, ter sua abrangência esclarecida de forma a que não seja prejudicial ao desenvolvimento de negócios e tecnologias.

3.5. Com relação ao artigo 7, §1°, o trecho "indispensáveis para a sua realização" é muito rígido e pode representar um obstáculo para o oferecimento de certos aplicações de internet. Não é raro que aplicações de internet requeiram que os usuários criem uma conta e forneçam certas informações pessoais para que estes possam ser acessados. Essas informações podem não ser necessariamente "indispensáveis" para o fornecimento daquelas aplicações (no sentido em que fornecer um endereço de entrega e faturamento é indispensável quando uma pessoa compra produtos online), mas ainda assim importantes para assegurar a identificação dos usuários, permitir que as aplicações forneçam o serviço de maneira mais eficiente e melhorar a qualidade do serviço, de forma geral. O mesmo raciocínio se aplica à big data analytics. Desde que os direitos de privacidade dos usuários sejam respeitados, requerer que dados sejam fornecidos para a prestação de determinado serviço não deveria ser proibido pela lei.

4. Consentimento dos Pais (Artigos 8 e 9)

4.1. Para menores entre doze e dezoito anos, ao mesmo tempo que apreciamos a intenção do anteprojeto, no sentido de que eles podem fornecer consentimento diretamente, determinar que tal consentimento poderá ser revogado pelos pais ou responsáveis legais a qualquer tempo gera incertezas que podem impedir os provedores de serviços de manter ou ampliar a variedade de aplicações online disponíveis para crianças. Além disso, essa exigência tornaria necessária a coleta de informações adicionais significativas, potencialmente de todos os usuários entre as idades de 12 e 18 anos, e talvez também dos pais, o que é contrário ao objetivo geral de minimizar a coleta de informações

pessoais. A complexidade envolvida na verificação e/ou autenticação da identidade dos pais e responsáveis legais dos usuários também poderia tornar as informações pessoais de crianças suscetíveis a fraudes e abusos.

4.2. Nós acreditamos que o Ministério da Justiça pode ajudar a expandir a variedade de serviços online dirigidos a crianças no Brasil criando exigências razoáveis de notificação e consentimento dos pais de crianças. Exigências excessivas teriam o efeito de desincentivar a criação de serviços voltados a crianças, deixando elas e seus pais sem outra alternativa a não ser serviços que não sejam voltados para crianças.

5. Consentimento (Artigo 10)

5.1. Adicionalmente aos comentários feitos aos artigos 5 e 7 acima, é importante considerar que espaço e funcionalidade são limitados em muitas aplicações de internet. Por essa razão, quando o consentimento é exigido, pode nem sempre ser possível fornecer as informações mencionadas no artigo 10 exatamente no momento em que este é solicitado (por mecanismos de opt in ou opt-out, por exemplo). Os provedores de serviços deveriam ser autorizados a fornecer esse tipo de informação separadamente aos titulares dos dados, em especial por meio de políticas de privacidade que possam ser acessadas online a qualquer tempo, como já é prática comum no mundo todo. Adicionalmente, pode ser difícil especificar a duração do tratamento de dados pessoais (conforme exigido no artigo 10, II). Em uma relação de prestação de serviços, é provável que os dados sejam tratados no mínimo enquanto o serviço estiver sendo prestado, mas pode não ser possível determinar isso no momento da coleta e diferentes tipos de dados podem ser tratados por períodos diferentes. Isso também torna difícil fornecer informações precisas e relevantes a esse respeito quando os dados são coletados. Além disso, o artigo 14 do projeto de lei já aborda os casos em que o tratamento de dados deve terminar.

5.2. Exigir que os titulares de dados sejam continuamente informados sobre a coleta de dados, conforme exigido no artigo 10, §4º, também é problemático e tem pouco efeito prático. O anteprojeto já requer que o consentimento seja renovado quando ocorrerem alterações a certas informações fornecidas aos titulares dos dados no ato da coleta; isso deveria ser suficiente para assegurar que os titulares dos dados sejam devida e continuamente informados sobre como seus dados são tratados.

6. Consentimento (Artigo 11)

6.1. Conforme comentado nos artigos 5 e 7 acima, o consentimento não deveria ser exigido quando o tratamento de dados representa um interesse comercial legítimo dos responsáveis, inclusive para fins de suportar as operações internas de um website ou de serviços online (por exemplo, garantir a segurança da rede e da informação, autenticação/prevenção de fraude ou o uso de data analytics para melhorar a oferta de serviços).

6.2. Com relação ao artigo 11, §1°, o conceito de retenção de dados pelo menor período de tempo possível é vago. Na nossa opinião, seria mais apropriado e eficaz determinar que dados devem ser tratados somente pelo período de tempo razoavelmente necessário para atingir a finalidade para a qual foram coletados.

7. Órgão Competente (Artigo 13)

7.1. O anteprojeto se refere em diversos artigos a um "órgão competente" que será responsável por estabelecer regras e regulamentações adicionais às obrigações estabelecidas pela lei. Apesar de que entendemos que regulamentação adicional pode ser necessária e que a lei pode não ser capaz de enunciar todos os detalhes relevantes, a lei deve identificar o órgão competente que terá essa tarefa e especificar o escopo de sua competência. É arriscado e ineficaz deixar uma gama tão ampla de questões para serem determinadas por um órgão não especificado com poderes não definidos.

8. Direitos do Titular de Dados (Artigo 18)

8.1. The immediate requirement in item (i) is impracticable and the seven-day term in item (ii) is extremely short. It would be more appropriate to determine that this information must be provided without undue delay or within a reasonable timeframe considering the nature and extent of the requested information.

9. Alocação de Responsabilidades (Artigos 22, 31 e 39)

9.1. A alocação de responsabilidade entre responsáveis, operadores de dados e cessionários deve ser revisada. O projeto de lei segue a abordagem de estabelecer

responsabilidade solidária entre todos esses agentes, o que pode ter consequências não desejadas no mercado de forma geral, em especial com relação a responsáveis e operadores de dados.

9.2. Na medida em que a lei atribui responsabilidade solidária aos operadores de dados, é razoável assumir que eles irão reavaliar o grau de risco de seus negócios no Brasil, o que, por consequência, pode afetar adversamente os negócios dos responsáveis pelos dados. Operadores de dados são em essência prestadores de serviços aos responsáveis pelos dados e a relação entre eles é de natureza privada, tipicamente regida por contratos privados. Ao estabelecer a responsabilidade solidária, a lei interfere nessa relação e pode desencorajar operações de tratamento de dados e a implementação de inovações no Brasil. A responsabilidade perante os titulares de dados deve ser dos responsáveis apenas, já que eles mantém relação direta com os titulares dos dados e tem condições de definir as medidas de proteção de dados mais adequadas, vis-à-vis as leis aplicáveis e seus próprios negócios, a serem observadas pelos operadores contratados por eles. Operadores de dados devem processar dados sob a responsabilidade dos responsáveis, que devem assegurar e ser capazes de demonstrar o cumprimento da lei.

9.3. Caso o Ministério da Justiça decida, todavia, seguir esse caminho, a lei deveria ser bastante clara no sentido de que esses dispositivos não afetam os acordos privados entre os responsáveis e os operadores de dados, em especial com relação às suas responsabilidades e direitos de indenização.

10. Transferência Internacional de Dados (Artigos 28, 29, 30, 31, 32 e 33)

10.1. Já que as exigências e restrições para transferência internacional de dados foram claramente inspiradas pelo modelo regulatório da União Europeia, é importante ressaltar que esse modelo tem deficiências e está atualmente sendo revisado.

10.2. A experiência da União Europeia mostrou que limitar a transferência internacional de dados para países com regras de proteção de dados semelhantes, conforme avaliado por uma autoridade governamental, é bastante oneroso tanto para as entidades privadas que fazem ou desejam fazer negócios na região quanto para as autoridades administrativas encarregadas de verificar o cumprimento dessa exigência. A intenção da lei brasileira deveria ser, na verdade, o oposto: assegurar um nível adequado de proteção à privacidade

sem criar obstáculos aos negócios no país, inclusive para empresas que tenham negócios globais. Um dos objetivos da revisão das regras de privacidade de dados da União Europeia atualmente em andamento é justamente simplificar e harmonizar o sistema de proteção de dados, inclusive com relação à transferência internacional de dados.

10.3. Caso o modelo da União Europeia deva ser seguido, acreditamos que, ao invés de estabelecer como regra a avaliação de adequação da legislação estrangeira e criar a necessidade de consentimentos adicionais para a transferência para outros países (conforme previsto no artigo 29), seria mais simples e eficiente estabelecer outros meios como alternativa à avaliação de adequação da jurisdição estrangeira para permitir a transferência internacional de dados. As cláusulas contratuais padrão ou normas corporativas globais (por meio das quais as empresas do mesmo grupo econômico podem expressar seu compromisso em fornecer e assegurar um nível de proteção de dados internacional adequado) mencionadas no artigo 30 são um exemplo disso, mas também exigem cautela no sentido de que para serem eficientes, o procedimento para aprovação de tais cláusulas ou normas pela autoridade governamental competente não pode ser burocrático ou lento (aprovações para transferências específicas, por exemplo, não atingiriam esse objetivo).

10.4. Na regulamentação deste tema, é importante ter em mente o ambiente dinâmico de desenvolvimento e oferta de serviços e aplicações de internet (inclusive computação na nuvem), o qual pode ser difícil refletir em uma regulamentação que imponha barreiras geográficas para a transferência de dados. Decisões sobre onde tratar e armazenar dados são em geral tomadas com base em parâmetros técnicos e limitar as empresas a fazê-lo pode ter um impacto negativo no mercado (como a experiência da União Europeia também demonstra).

11. Encarregado pelo Tratamento de Dados Pessoais (Artigo 41)

11.1. O emprego e indicação de um encarregado pelo tratamento de dados pessoais não deveria ser obrigatório. Questões de estrutura organizacional e atribuições de responsabilidades tornam ineficiente a exigência por um único ponto de contato. No caso de grandes empresas, isso irá criar um gargalo, possivelmente atrasando respostas e enfraquecendo comunicações de boas vindas. Pequenas empresas comumente não possuem recursos para alocar uma única pessoa em uma mesma posição por tempo integral.

12. Incidente de Segurança (Artigos 44 e 45)

12.1. A obrigação de comunicação estabelecida no artigo 44 é vaga e pode resultar em incerteza sobre quais são os incidentes de segurança que devem ser comunicados e/ou em perturbações desnecessárias dos negócios para as empresas e sobrecarregamento de autoridades governamentais. Um critério mais objetivo para definir a comunicação de incidentes de segurança deve ser estabelecido: sugerimos que apenas incidentes envolvendo dados sensíveis não criptografados ou não ofuscados ou que sejam prováveis de causar prejuízo financeiro sejam de comunicação obrigatória. Comunicação imediata também não é viável; seria mais razoável exigir que a comunicação seja feita sem demora injustificada.

12.2. A obrigação no artigo 45, §2º de informar os titulares de dados pessoais sempre que um incidente coloque em risco a segurança dos dados ou possa causar danos ao titular dos dados também deve ser revisada para incluir critérios mais objetivos. Em princípio, qualquer incidente constitui um risco para a segurança dos dados e tem o potencial de causar algum dano – mas a probabilidade disso acontecer, na prática, deve ser avaliada caso a caso. Com a redação atual, informar os titulares de dados se tornaria uma regra sempre que um incidente, relevante ou não, ocorrer. Exigir notificação mesmo para incidentes que não causem prejuízos pode gerar descaso com relação às notificações e levar os titulares de dados a ignorar notificações de incidentes.

Nós agradecemos a oportunidade de oferecer nossos comentários ao Anteprojeto e esperamos continuar trabalhando com o Ministério da Justiça durante o processo de elaboração de uma legislação para proteção de dados pessoais no Brasil.

Atenciosamente,

Entertainment Software Association

_____

Nome: Stanley Pierre-Louis

Cargo: Senior Vice President & General Counsel