RIO DE JANEIRO 2015

Anteprojeto de lei de proteção de dados pessoais/ *Contribuição do ITS para o debate público*

Instituto
de Tecnologia
& Sociedade
do Rio

Resumo

Esta é uma contribuição do ITS ao debate público sobre o anteprojeto de lei de dados pessoais, realizada pela Secretaria de Assuntos Legislativos e pela Secretaria Nacional do Consumidor, do Ministério da Justiça, em 2015. A contribuição do ITS centra-se nos seguintes pontos: jurisdição; Dados Anônimos versus Finalidade; Autoridade de Garantia; dados público de acesso irrestrito versus consentimento versus finalidade; Consentimento como forma de legitimação de um tratamento de dados pessoais; e Tratamento de dados necessário a atender os interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados..

Rio de Janeiro, 5 de Julho de 2015.

1/ Jurisdição

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:

I – a operação de tratamento seja realizado no território nacional; ou

II – os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

§1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

Comentário:

O âmbito de aplicação material do APL, para abarcar toda e qualquer operação de tratamento realizada por meio total ou parcialmente automatizado, não importando o local da sede do responsável ou operador, resolve um problema enfrentado pela Diretiva Europeia 95/46/CE, que não previu de forma expressa que o âmbito de aplicação não dependia da sede do responsável ou operador, nem da localização do banco de dados.

Já o âmbito de territorial proposto pelo APL (incisos I e II do art. 2º) merece reflexão. O primeiro ponto diz respeito ao que se considera como dados coletados no território nacional. O §1º do art. 2º dispõe que seriam aqueles dados pessoais coletados no território nacional **quando o titular nele se encontre no momento da coleta**. Essa previsão, além de limitar o âmbito de atuação da futura legislação, gera alguma confusão e insegurança jurídica, já que se criará um ônus adicional aos responsáveis e operadores de tratamentos de dados para verificarem, no momento da coleta, se o titular dos dados se encontra no país. Isso porque os dados pessoais, muitas vezes, não são coletados diretamente de seu titular, o que torna essa verificação ainda mais complexa. Uma alteração no texto que talvez afastasse essa dúvida seria incluir no §1º que "**também** se consideram como coletados no território nacional, para os fins desta Lei, os dados pessoais cujo titular nele se encontre no momento da coleta".

Essa alteração, entretanto, nos levaria a outro dilema. Pela leitura conjunta do inciso II do art. 2º com o §1º do mesmo artigo, podemos chegar à interpretação de que qualquer tratamento de dados realizado a partir de um titular situado no Brasil seria alcançado pela futura lei, o que não parece ser a melhor solução. Uma alternativa que vem sendo debatida no âmbito do processo de revisão da legislação sobre proteção de dados na União Europeia (art. 3º (2) Proposta de Regulamento Geral sobre Proteção de Dados) é de se vincular a aplicação da lei a tratamentos de dados efetuados no exterior, a partir de um titular situado no país submetido a determinada lei de proteção de dados, ao fato de esse tratamento estar relacionado com: a) A oferta de bens ou serviços a esses titulares de dados; ou b) O controle/monitoramento de seu comportamento (na rede, por exemplo). Ora, a ideia de poder aplicar a lei a tratamentos de dados efetuados no exterior é de proteger o titular nas hipóteses em que a 'coleta' foi direcionada a ele, por exemplo um serviço em português oferecido por um site estrangeiro e voltado para o público brasileiro.

2/ Dados anônimos versus finalidade

Art. 5º

IV – dados anônimos: 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;

Comentário:

O ponto que merece reflexão é o que se refere ao "conjunto de meios suscetíveis de serem razoavelmente utilizados para identificar" o titular do dado. Diversas pesquisas acadêmicas têm demonstrado que a re-identificação de um titular de dados a partir de dados anônimos ou anonimizados (dissociados) têm se tornado uma tarefa cada dia mais fácil, barata e rápida. Assim, não nos parece que o fato de um dado poder ou não ser re-identificado seja o ponto primordial para a não incidência da futura lei de proteção de dados. A discussão faria muito mais sentido se levasse em consideração a finalidade do tratamento de dados que se pretende realizar e dos mecanismos utilizados para impedir/dificultar a identificação dos titulares dos dados, por exemplo o uso de criptografia. A discussão que queremos propor é de que não é o fato de o titular de determinado ser ou não identificável, mas sim a finalidade do tratamento de tal dado e os mecanismos utilizados para dificultar essa identificação.

Apenas para auxiliar no debate, a proposta de Regulamento Geral de Proteção de Dados em discussão na União Europeia propõe que o dado para ser anônimo devem ser considerados "os meios com razoável probabilidade de serem utilizados pelo responsável pelo tratamento ou por qualquer outra pessoa singular ou coletiva", ou seja, não se trata aqui simplesmente de possibilidade de re-identificação do titular do dado, mas sim de probabilidade real e razoável de que essa re-identificação venha a ser tentada.

Outra alternativa seria adotar o entendimento de que os tratamentos de dados pessoais que tivessem sido submetidos a algum processo de dissociação (anonimização) estariam dispensados de algumas exigências da futura lei, como por exemplo atender a pedidos de acesso e demais direitos dos titulares dos dados. Nesse caso o processo de dissociação deveria ser reconhecido como válido pela Autoridade de Proteção de Dados.

3/ Autoria de garantia

Comentário:

Um ponto que também merece atenção diz respeito à autoridade competente para fiscalizar o cumprimento da futura lei de proteção de dados. O APL se refere a 'órgão competente', o que nos remete a um órgão dentro da hierarquia da administração direta, sem a independência necessária que uma autoridade de proteção de dados necessita, especialmente quando ela também fiscalizará órgãos da própria administração direta à qual ela estará vinculada.

Parece-nos, assim, que a melhor solução seria a criação de uma agência de proteção de dados, no formato de uma agência reguladora, com independência financeira e administrativa e com mandato fixo para os seus diretores. Essa agência, futuramente, poderia também englobar competências relacionadas a outros temas, como a Lei de Acesso à Informação. Esse, aliás, foi o modelo adotado por todos os países membros da União Europeia.

4/ Dados públicos de acesso irrestrito *versus* Consentimento *versus* Finalidade

Comentário:

O §1º do art. 11 do APL dispensa a exigência do consentimento do titular de dados quando o tratamento envolver 'dados públicos de acesso irrestrito'. Essa previsão apresenta, à primeira vista, dois problemas. O primeiro deles em se saber o que seriam 'dados irrestritos de acesso público', já que o APL, apesar de se referir a eles, não traz uma definição do que seriam. O outro pronto diz respeito à possibilidade de tratamento desses dados pelo simples fato de serem disponíveis ao público. Será que os dados do bolsa família, apenas para usar um exemplo relevante, poderiam ser tratados para fins de concessão de crédito, ou seja, os agentes financeiros, valendo-se desses dados que têm um acesso irrestrito ao público, poderiam trata-los, independente do consentimento de seus titulares para este fim? O mesmo com relação aos vencimentos dos servidores públicos, que passaram a ser divulgados na internet? Entendemos que no tratamento de dados pessoais, mesmo que de 'acesso irrestrito' devem observar certos limites, e um deles é justamente o princípio da finalidade. Assim, ainda que essa dispensa de consentimento prevalece, deve ficar claro que apesar disso o responsável pelo tratamento deverá observar os demais ditames previstos na futura lei, em especial o princípio da finalidade, não podendo o dado ser tratado para uma finalidade incompatível com aquela para a qual o dado foi tratado inicialmente.

5/ Consentimento como forma de legitimação de um tratamento de dados pessoais

Comentário:

O consentimento do titular é usualmente tratado como um requisito essencial para o tratamento de dados pessoais, justamente para que se demonstre a existência de um relacionamento entre o titular e o responsável capaz de justificar o tratamento de dados daquele. Todavia, no ambiente virtual e em especial nas situações relacionadas ao big data e ao *cloud computing,* muitas vezes se mostra difícil, se não impossível, atender plenamente aos requisitos relativos à obtenção de um consentimento válido, podendo, inclusive, inviabilizar algumas atividades hoje exercidas na web. Por isso, acreditamos que nessas situações poderia ser buscada uma solução que se valesse menos do consentimento, da forma como ele foi concebido no APL, para se concentrar em outras garantias dos titulares dos dados, como a possibilidade de acesso, correção, bloqueio ou mesmo cancelamento de seus dados, buscando-se, nesses casos, um modelo restrito com base no opt-out ao invés do modelo tradicional de opt-in de consentimento.

6/ Tratamento de dados necessário a atender os interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados

Comentário:

Uma importante hipótese de tratamento de dados pessoais contida na maioria das leis gerais de proteção de dados - para não dizer em todas - ficou ausente da relação contida no artigo 11 do APL. É a hipótese de tratamento de dados necessário ao atendimento dos interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados. Essa base legal está prevista na Diretiva 95\46\CE, em seu artigo 7º (f):

Artigo 7º - Os Estados-membros estabelecerão que o tratamento de dados pessoais só poderá ser efetuado se:

f) O tratamento for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa, protegidos ao abrigo do nº 1 do artigo 1º

Essa opção ao consentimento coloca de um lado os interesses e direitos do titular dos dados e de outro os legítimos interesses do responsável pelo tratamento (ou de terceiros) devendo ser realizada, caso a caso, uma ponderação de interesses para se verificar se no caso concreto o interesse de um ou outro irá prevalecer.

Essa hipótese de autorização ao tratamento de dados é de vital importância para se possibilitar a realização de tratamentos de dados legítimos, mas que seriam dificilmente enquadrados nos sete incisos do art. 11 do APL, em hipóteses nas quais o consentimento não seria uma base legal adequada.

O Grupo de Trabalho do Artigo 29, grupo composto por representantes das autoridades de proteção de dados pessoais dos países membros da União Europeia, representantes da Autoridade Europeia de Proteção de Dados e da Comissão da União Europeia, já se manifestou acerca do conceito de legítimo interesse para fins da Diretiva, bem como das situações em que é possível aplicar referido item "f", em seu "Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na acepção do artigo 7.º da Diretiva 95/46/CE".

Neste sentido, o Grupo de Trabalho do Artigo 29 entende que "um interesse pode ser

considerado legítimo desde que o responsável pelo tratamento possa prosseguir esse interesse em conformidade com a legislação em matéria de proteção de dados e a demais legislação aplicável, ou seja, um interesse legítimo deve ser «admissível nos termos da lei»"(Grupo de Trabalho do Artigo 29. Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na acepção do artigo 7.º da Diretiva 95/46/CE. P. 39).

Na linha do que prevê a Diretiva Europeia sobre proteção de dados pessoais o interesse é legítimo quando: (i) é lícito, (ii) é definido de forma suficientemente clara para permitir a realização do teste da ponderação em relação aos interesses e aos direitos fundamentais da pessoa em causa, e (iii) representa um interesse real e atual. Esse teste de ponderação leva em consideração os seguintes fatores: a) avaliação do interesse legítimo do responsável pelo tratamento, i.e, se os interesses envolvem direitos fundamentais ou coincidem com interesses públicos, b) impacto do tratamento sobre o titular do dado, c) o cumprimento pelo responsável pelo tratamento das exigências constantes da Diretiva; e d) a adoção pelo responsável pelo tratamento de medidas adicionais de proteção. A Diretiva cria o chamando "teste da ponderação" entre o interesse envolvido e os direitos dos titulares dos dados, para analisar a possibilidade de invocar o legítimo interesse previsto no item "f" como fundamento para o tratamento de dados pessoais.

Assim, propomos que seja incluído no art. 11 do APL novo inciso para contemplar essa hipótese. Porém, referido dispositivo deve estabelecer, de forma expressa, que a ponderação dos interesses envolvidos deve levar em conta os seguintes fatores:

- A natureza e a fonte do interesse legítimo e se o tratamento de dados e necessário para o exercício de direitos fundamentais ou se é feito no interesse público ou, ainda, se seus benefícios recebem reconhecimento da sociedade;
- O impacto nos direitos do titular dos dados e quais seriam as suas legítimas expectativas com relação ao que será feito com os seus dados, além da natureza dos dados tratados - se sensíveis ou não - e como serão tratados;
- As medidas adotadas pelo responsável pelo tratamento para minimizar o impacto na privacidade do titular dos dados, sejam tecnológicas, em termos de políticas de privacidade ou mesmo de transparência.

Uma possível redação, que vai na mesma direção da sugestão apresentada pelo Grupo de Trabalho do Artigo 29 em seu parecer sobre a noção de legítimo interesse do responsável pelo tratamento no que toca ao art. 7º da Diretiva 95\46\CE seria a seguinte:

- Tratamento necessário ao atendimento de interesses legítimos do responsável pelo tratamento, desde que não prevaleçam interesses e direitos do titular do dado, considerando-se a natureza e a fonte do interesse legítimo, a existência de um interesse público relevante a autorizar o tratamento e o impacto nos direitos dos titulares dos dados.