Comentários sobre o Anteprojeto de Lei de Proteção de Dados Pessoais

Rodrigo Veleda

5 de julho de 2015

Sumário

1 Descrição

Rodrigo Veleda é o editor do blog Não Sou Um Número[1], dedicado ao debate sobre questões de privacidade e, em menor escala, liberdade de informação no setor público.

2 Comentários

O anteprojeto já no seu artigo 4º tem uma cláusula controversa:

> Art. 4º Os tratamentos de dados pessoais para fins exclusivos de segurança pública, defesa, segurança do Estado, ou atividades de investigação e repressão de infrações penais, serão regidos por legislação específica, observados os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

Esta é a famosa cláusula NSA, que permite que órgãos de segurança e inteligência desconsiderem a lei de proteção de dados pessoais em favor de qualquer lei específica.

E não são apenas as atividades de segurança pública e segurança do Estado que têm amplas liberdades em relação a este anteprojeto. O artigo 6º fala dos princípios, eis que temos o parágrafo 2º:

[1] http://naosouumnumero.blogspot.com/

> § 2º O uso compartilhado de dados pessoais deve atender a finalidade específica de execução de políticas públicas e atribuição legal pelos órgãos e entidades públicas, respeitando o princípio da finalidade, adequação e necessidade dispostos nos incisos I, II e III.

Para variar, temos o uso dum termo esotérico, "políticas públicas", que, invariavelmente, abrigará qualquer coisa executada por ente público ou a mando deste. Pois bem, sabes quais os princípios que a execução de políticas públicas não precisará seguir? Transcrevo-os:

> IV – princípio do livre acesso, pelo qual deve ser garantida consulta facilitada e gratuita pelos titulares sobre as modalidades de tratamento e sobre a integralidade dos seus dados pessoais;
>
> V – princípio da qualidade dos dados, pelo qual devem ser garantidas a exatidão, a clareza e a atualização dos dados, de acordo com a periodicidade necessária para o cumprimento da finalidade de seu tratamento;
>
> VI – princípio da transparência, pelo qual devem ser garantidas aos titulares informações claras e adequadas sobre a realização do tratamento;
>
> VII – princípio da segurança, pelo qual devem ser utilizadas medidas técnicas e administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
>
> VIII – princípio da prevenção, pelo qual devem ser adotadas medidas capazes de prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; e
>
> IX – princípio da não discriminação, pelo qual o tratamento não pode ser realizado para fins discriminatórios.

Ou seja, para executar uma política pública, não precisará dar acesso gratuito aos titulares da informação, não será necessária manter a qualidade dos dados, transparência é algo que vai para o espaço, os dados não precisarão estar seguros, e, por consequência, não há necessidade de prevenção e discriminação pode ser utilizada.

Continuando, nós temos o art. 7º, que diz que o tratamento de dados pessoais só será feito com consentimento, seguido pelos arts. 8º, 9º e 10, que versam sobre o consentimento. Eis que vem o art. 11, com as exceções que permitem o tratamento de dados sem consentimento:

> Art. 11. O consentimento será dispensado quando os dados forem de acesso público irrestrito ou 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.

§ 1º Nas hipóteses de dispensa de consentimento, os dados devem ser tratados exclusivamente para as finalidades previstas e pelo menor período de tempo possível, conforme os princípios gerais dispostos nesta Lei, garantidos os direitos do titular.

§ 2º Nos casos de aplicação do disposto nos incisos I e II, será dada publicidade a esses casos, nos termos do parágrafo 1º do art. 6º.

§ 3º No caso de descumprimento do disposto no §2o, o operador ou o responsável pelo tratamento de dados poderá ser responsabilizado.

No começo do artigo 11 temos mais um termo esotérico, os tais dados de "acesso público irrestrito", definição esta que não se encontra no tal anteprojeto de lei. Daí temos as exceções nos casos que não envolvem dados de "acesso público irrestrito".

O primeiro caso é o cumprimento de obrigações legais. Evidentemente que a lei nada fala da criação de obrigações legais, se dar-se-á por lei, se haverá estudos de impacto de privacidade, nada! É mais outro termo esotérico. E chegamos no segundo caso, que ainda é pior, pois permite o compartilhamento de dados bastando haver apenas um regulamento da administração pública, sem a necessidade de discussão no Legislativo. O terceiro caso fala de cumprimento de obrigações contratuais, o que pode dar margem para o descumprimento dos princípios. O quarto caso é uma das aberrações deste projeto pois permite o acesso a dados pessoais bastando haver uma "pesquisa histórica, científica ou estatística" mesmo sem a dissociação de dados pessoais; algo um tanto inócuo já que é possível identificar pessoas usando[2] dados de transações de cartões de crédito mesmo que não haja dados como nome, endereço, número do cartão e semelhantes. Ou ainda, como em 1990 já era possível identificar[3] a maioria da população americana com os dados dissociados do censo daquele país. Isto para não falar na confusa hipótese do "sempre que possível".

[2]Hardesty, Larry. "Privacy Challenges." MIT News. MIT News Office, 29 Jan. 2015. Web. 05 Jul. 2015. <http://newsoffice.mit.edu/2015/identify-from-credit-card-metadata-0129>.

[3]Perry, Caroline. "You're Not so Anonymous." Harvard Gazette. SEAS Communications, 18 Oct. 2011. Web. 05 July 2015. <http://news.harvard.edu/gazette/story/2011/10/you%E2%80%99re-not-so-anonymous/>.

Seguindo, nós temos a possibilidade de dispensa de consentimento em processo judicial, nada muito a acrescentar pois é um terceiro que determinará o acesso ao dado pessoal; pois depois vem o problema, haverá dispensa de consentimento em processo administrativo. Traduzido para o português, basta que haja um processo administrativo que teus dados estarão disponíveis. A próxima possibilidade de dispensa de consentimento é para "proteção da vida ou da incolumidade física do titular ou de terceiro", exemplo, se um alguém precisar de "proteção da vida", teus dados podem ser acessados, se o operador julgar necessário. E a última possibilidade é a tal "tutela da saúde", outro termo que não possui nenhuma definição na lei, onde basta ser um profissional da área da saúde ou ser membro duma entidade sanitária para poder acessar dados pessoais sem consentimento. E se isto tudo não fosse suficiente, o parágrafo 3º diz que o operador ou responsável poderá ser punido, isto é, não há sequer a obrigatoriedade de punição, em caso de descumprimento do parágrafo 2º.

E vamos para o artigo 12, que fala sobre o acesso aos dados pessoais sensíveis. Antes de adentrar no artigo 12, eu transcrevo a definição de dado pessoal sensível:

> III – dados sensíveis: dados pessoais que revelem a origem racial ou étnica, as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, bem como dados genéticos;

Isto é importante de citar pois o inciso II do artigo 12 prevê a hipótese de dados pessoais sensíveis de acesso público irrestrito; por exemplo, não seria absurdo para esta lei de proteção de dados pessoais a existência de um banco de dados público de acesso irrestrito sobre a tua vida sexual ou divulgando teu código genético. E não me repetirei nas hipóteses de acesso aos dados pessoais sensíveis sem consentimento do titular, do tipo, se alguém quiser fazer uma pesquisa histórica, científica ou estatística com teu prontuário médico, tu não podes fazer nada, já que teu consentimento é desnecessário. E de brinde, tu tens isto:

> § 2º O tratamento de dados pessoais biométricos será disciplinado por órgão competente, que disporá sobre hipóteses em que dados biométricos serão considerados dados pessoais sensíveis.

Sim, a biometria pode ser um dado sensível ou não, talvez para atender a sugestão[4] da Equifax na primeira consulta ao tal anteprojeto. Relembrando que o anterior anteprojeto de proteção de dados pessoais considerava dados biométricos como dados pessoais sensíveis, muito embora isto não desse muita proteção

[4]Equifax do Brasil Ltda. "Comentários e Sugestões Acerca do Anteprojeto sobre Proteção de Dados Pessoais." (n.d.): n. pag. Abr. 2011. Web. 5 Jul. 2015. <http://culturadigital.br/dadospessoais/files/2011/04/Coment%C3%A1rios-e-Sugest%C3%B5es-Acerca-do-Anteprojeto-sobre-Prote%C3%A7%C3%A3o-de-Dados-Pessoais-Equifax-para-incluir-no-site.pdf>.

ao dado... Falando no anteprojeto anterior, as hipóteses de desconsideração de consentimento eram menos abrangentes do que as atuais.

A seguir, o anteprojeto fala em cancelamento dos dados pessoais, lembrando que a definição de cancelamento é omissa em relação a backups. E lá vamos com o artigo 15:

> Art. 15. Os dados pessoais serão cancelados após o término de seu tratamento, autorizada a conservação para as seguintes finalidades:
>
> I – cumprimento de obrigação legal pelo responsável;
>
> II – pesquisa histórica, científica ou estatística, garantida, sempre que possível, a dissociação dos dados pessoais; ou
>
> III – cessão a terceiros, nos termos desta Lei.
>
> Parágrafo único. Órgão competente poderá estabelecer hipóteses específicas de conservação de dados pessoais, garantidos os direitos do titular, ressalvado o disposto em legislação específica.

Mas antes, a definição de cancelamento:

> XVI – cancelamento: eliminação de dados ou conjunto de dados armazenados em banco de dados, seja qual for o procedimento empregado;

Como eu disse, nada de backup. E eis que surge a novilíngua: a eliminação de dados significa cessão a terceiros. Traduzindo, ao invés de teus dados serem eliminados, eles serão cedidos a um terceiro. E claro, nós temos a "pesquisa histórica, científica ou estatística". E sem contar na expressão "legislação específica".

Mas nós também temos direitos.

> Art. 17. O titular dos dados pessoais tem direito a obter:
>
> (...)
>
> §1º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, alegando descumprimento ao disposto nesta Lei.

Tu não entendeste? Eu também não! Ora, se justamente a dispensa de consentimento existe para que o titular do dado não possa se opor ao tratamento do dado, como ele pode opor-se ao tratamento? E que descumprimento seria esse, se a lei permite o tratamento com dispensa de consentimento. Isto não faz sentido algum. E nós temos um artigo potencialmente caro no anteprojeto:

> Art. 18. A confirmação de existência ou o acesso a dados pessoais serão providenciados, a critério do titular:
>
> (...)
>
> § 2º As informações e dados poderão ser fornecidos, a critério do titular:
>
> (...)

> II – sob a forma impressa, situação em que poderá ser cobrado exclusivamente o valor necessário ao ressarcimento do custo dos serviços e dos materiais utilizados.

Explico. Se tu fores uma pessoa que não tem acesso a meios eletrônicos, tu terás que pagar para saber se estão a utilizar teus dados pessoais, independentemente do fato do operador estar ganhando dinheiro com teus dados.

Depois, temos o artigo 24:

> Art. 24. A comunicação ou interconexão de dados pessoais entre pessoa jurídica de direito público e pessoa de direito privado dependerá de consentimento livre, expresso, específico e informado do titular, salvo:
>
> I – nas hipóteses de dispensa do consentimento previstas nesta Lei;
>
> II – nos casos de uso compartilhado de dados previsto no inciso XVII do art. 5º, em que será dada publicidade nos termos do §1º do art. 6º; ou
>
> III – quando houver prévia autorização de órgão competente, que avaliará o atendimento ao interesse público, a adequação e a necessidade da dispensa do consentimento.
>
> Parágrafo único. A autorização prevista no inciso III do caput poderá ser condicionada:
>
> I – à comunicação da interconexão aos titulares, nos termos do §1º do art. 6º;
>
> II – ao oferecimento aos titulares de opção de cancelamento de seus dados; ou
>
> III – ao cumprimento de obrigações complementares determinadas por órgão competente.

Claro, qualquer ente estatal poderá interconectar-se com uma base de dados privada por qualquer motivo, já que temos várias hipóteses de dispensa de consentimento. E olha o que se alude o inciso II:

> XVII – uso compartilhado de dados: a comunicação, a difusão, a transferência internacional, a interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos, no cumprimento de suas competências legais, ou entre órgãos e entidades públicos e entes privados, com autorização específica, para uma ou mais modalidades de tratamento delegados por esses entes públicos;

Temos dois termos não definidos, "competências legais" e "autorização específica". E ainda temos a transferência internacional destes dados. Continuando com a análise do artigo 24, temos o inciso III que permite ao órgão competente dispensar o consentimento no improvável caso de não se ter achado brechas no inciso I e II. E se isto não bastasse, o parágrafo único diz que poderá, e não

deverá, ter condicionantes para aplicação do inciso III. Ou seja, o órgão competente poderá dispensar a comunicação da interconexão e poderá dispensar o oferecimento do cancelamento.

E já que citamos transferências internacionais, o anteprojeto de lei também tem um artigo só para este caso:

> Art. 28. A transferência internacional de dados pessoais somente é permitida para países que proporcionem nível de proteção de dados pessoais equiparável ao desta Lei, ressalvadas as seguintes exceções:
>
> I – quando a transferência for necessária para a cooperação judicial internacional entre órgãos públicos de inteligência e de investigação, de acordo com os instrumentos de direito internacional;
>
> II – quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> III – quando órgão competente autorizar a transferência, nos termos de regulamento;
>
> IV – quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
>
> V – quando a transferência for necessária para execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do §1º do art. 6º.

Já começamos com um inciso NSA, que permite a transferência de dados para o estrangeiro para órgãos de inteligência sem o consentimento do titular. Desta vez não há a cláusula da "pesquisa histórica, científica ou estatística". Para variar, a lei permite que o órgão competente autorize a transferência de dados pessoais para o estrangeiro por mera decisão administrativa interna deste órgão. O antigo anteprojeto, no artigo 35, era um pouco mais restrito; esta versão é bem menos restritiva. E a identificação de tais transferências é uma mera possibilidade, não uma obrigação do órgão competente, conforme artigo 33.

> Art. 33. Órgão competente poderá estabelecer normas complementares que permitam identificar uma operação de tratamento como transferência internacional de dados pessoais.

E depois de tudo isso o anteprojeto de lei vem falar em responsabilidades no setor público:

> Art. 37. As punições cabíveis no âmbito desta Lei serão aplicadas pessoalmente aos operadores e responsáveis de órgãos públicos que agirem de forma contrária a esta Lei, conforme disposto na Lei no 8.112, de 11 de dezembro de 1990 e na Lei no 8.429, de 2 de junho de 1992.
>
> Art. 38. As competências e responsabilidades relativas à gestão de bases de dados nos órgãos e entidades públicos, bem como a responsabilidade pela prática de atos administrativos referentes a dados pessoais, serão definidas nos atos normativos que tratam da definição de suas competências.

A Lei 8112/1990, vulgo Estatuto do Servidor Público Federal, nada fala em seu capítulo de proibições sobre o assunto. A Lei 8429/1992, a Lei de Improbidade Administrativa, até fala no assunto:

> Art. 11. Constitui ato de improbidade administrativa que atenta contra os princípios da administração pública qualquer ação ou omissão que viole os deveres de honestidade, imparcialidade, legalidade, e lealdade às instituições, e notadamente:
> (...)
> III - revelar fato ou circunstância de que tem ciência em razão das atribuições e que deva permanecer em segredo;

Embora seja discutível o que significa segredo, uma vez que isso pode ser relativo a classificação de dados sigilosos do governo, e não dados pessoais. E o artigo 38, mais uma vez, joga para qualquer outra legislação a responsabilidade dos agentes públicos com relação aos dados pessoais.

E numa hipótese de que dados pessoais sejam divulgados em desacordo com esta lei, o artigo 45 dá ampla liberdade, sem obrigatoriedade, para o órgão competente agir:

> 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; ou
> III – medidas para reverter ou mitigar os efeitos de prejuízo.

Este anteprojeto sequer obriga a adoção de medidas para reversão ou comunicação aos titulares, estando estes à mercê do órgão competente. Por exemplo, se um site de exames médicos estiver disponibilizando dados pessoais sensíveis, a pronta comunicação dos titulares e/ou a adoção de medidas de reversão dependerá única e exclusivamente da vontade do órgão competente, já que a lei não traz tal obrigação.

E se nós chegarmos a possibilidade de sanções, lembra-te que os agentes públicos não estão sujeitos à multa. Mas não te preocupas, que o parágrafo 4º diz que as sanções administrativas em nada prejudicam as sanções administrativas, civis e penais das legislações específicas. O projeto sequer é capaz de definir as sanções as violações de seu próprio texto. Eu quero saber onde acho a punição por coletar dados desnecessários, qual a punição para que não cancela dados e por aí vai.

3 Sugestões

1. Condicionar a coleta de dados pessoais por órgãos e entidades públicas à uma prévia autorização do poder legislativo, ou seja, via projeto de lei, em que se especifique que dados serão coletados, sua finalidade, quem

poderá acessá-los e tratá-los e os prazos para manutenção de tais dados em arquivo;

2. Proibir o acesso a dados pessoais sensíveis, sem o consentimento do titular, que não por meio de ordem judicial;

3. Fazer, que sempre que o possível, obrigatório o uso de ordem judicial para acesso a dados pessoais que não são classificados como sensíveis;

4. Definir o conceito de dado pessoal de acesso público irrestrito como aqueles dados pessoais que não permitam acesso a outros bancos de dados com outros dados pessoais ou dados pessoais sensíveis;

5. Definir como padrão no Brasil o opt-in[5];

6. Fazer do uso de informações biométricas de vontade exclusiva das pessoas a quais tais dados se referem, proibindo que entes públicos e privados condicionem o acesso a bens, produtos e serviços a coleta de dados biométricos;

7. Exigir data para cancelamento automático de dados, respeitando prazos contratuais e estabelecidos por meio de lei;

8. A transferência de dados pessoais entre os diferentes Poderes e Entes Federativos dependerá de prévia autorizaçao legislativa do ente que coletou os dados;

9. A transferência internacional de dados sem o consentimento do titular só poderá ser autorizada pela Justiça Federal;

10. Obrigação da elaboração de Estudos de Impacto de Privacidade para as pessoas naturais e jurídicas de direito privado, quando estas tratarem dados pessoais sensíveis, e para as pessoas jurídicas de direito público, quando estes tratarem quaisquer tipos de dados pessoais;

11. Criar tipos penais para os agentes públicos que divulgarem dados pessoais ou que exigirem dados pessoais sem autorização legal, idem para pessoas naturais e jurídicas de direito privado;

12. Exigir o registro, no órgão competente, das pessoas que lidarão com dados pessoais sensíveis, exceto nas situações em que esta pessoa não tenha como copiar para si tal dado pessoal sensível e

13. Estimular as boas práticas entre os mais variados Entes Federativos e Poderes por meio de conferências anuais, troca de ideias e outras práticas que possam criar um melhor ambiente para a proteção de dados pessoais no Brasil.

[5]The Office of the CISO. "Privacy Brief: Opt In Versus Opt Out." University of Washington, n.d. Web. 5 Jul. 2015. <http://http://ciso.washington.edu/resources/privacy-briefs/privacy-brief-opt-in/>