EMENDA Nº ....., de 2015 - CCT
(AO PROJETO DE LEI DO SENADO Nº 330, DE 2013)

Inclua-se como Seção V, do Capítulo III – Do Regime Jurídico do Tratamento de Dados Pessoais –, do Projeto de Lei do Senado nº 330, de 2013, a qual constará com a seguinte redação:

"SEÇÃO V

Da Responsabilidade Demonstrável

Art. 29. Na aplicação pelo responsável do princípio indicado no inciso X do art. 4º desta Lei, este deverá:

I - implementar programa de governança em privacidade que, no mínimo:

a) demonstre o comprometimento do responsável em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo em que se deu sua coleta;

c) seja adaptado à estrutura, escala e volume de suas operações, bem como à sensibilidade dos dados tratados;

d) estabeleça políticas e salvaguardas adequadas a partir de processo de avaliação sistemática de impactos e riscos à privacidade;

e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) esteja integrado à sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

g) conte com planos de resposta a incidentes e remediação;

h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

II – estar preparado para demonstrar a efetividade de seu programa de governança de privacidade quando apropriado, e em especial, a pedido da autoridade administrativa competente ou de outra entidade responsável por promover o cumprimento boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei." (NR)

JUSTIFICAÇÃO

Os bancos de dados que contêm informações que dizem respeito a cidadãos, consumidores, segurados, bancarizados, pacientes, ou seja, a cada um de nós nas diversas personas que adotamos ou que nos são impostas em nossas relações sociais, existem pelo menos há tanto tempo quanto existem sistemas de computação (mesmo em seus primórdios, como sistemas mecânicos e eletromecânicos).

Foi a partir da década de 1960[1], na qual, não por acaso, deu-se a adoção cada vez mais difundida dos então poderosíssimos *mainframes* que a questão da proteção de dados passou a figurar como questão fundamental de política pública.

Leis e normas supranacionais a esse respeito surgiram logo depois, na segunda metade da década de 1970. Já em 1978, houve bastante interesse no tema da proteção de dados, particularmente sobre como a proteção conferida aos titulares dos dados poderia vir a afetar o livre fluxo de informações entre fronteiras.

Foi nesse contexto que a Organização para a Cooperação e Desenvolvimento Econômico - OCDE - criou uma força-tarefa com a missão de estudar o tema. Resultaram desse trabalho as "OECD Privacy Guidelines" (Diretrizes para Privacidade da OCDE) adotadas pela organização em 1980, constituindo base para a maioria das leis de proteção de dados que se seguiram.

[1] Vide obras de seminais de Alan F. Westin, Privacy and Freedom (1967) e Arthur Miller, Assault on Privacy, Computers, Data Banks and Dossiers (1971).

Em apertadíssimo resumo, as Diretrizes refletiam de forma bastante explícita a ideia de que a proteção de dados depende da estruturação de uma cadeia de controle na qual o indivíduo, ou titular dos dados, ocupa papel de protagonismo. Símbolo dessa noção é o conceito de "autodeterminação informativa", o qual designa o direito dos titulares dos dados de "decidirem por si próprios quando, como e dentro de quais limites informações que digam respeito a estes será comunicada a terceiros".

Foi nesse paradigma que as Diretrizes estabeleceram oito princípios fundamentais para justificar o uso e processamento justo de dados pessoais, quais sejam:

(i) princípio de limitação da coleta;
(ii) princípio de qualidade dos dados;
(iii) princípio da definição da finalidade;
(iv) princípio da limitação de utilização;
(v) princípio do back-up de segurança;
(vi) princípio da abertura;
(vii) princípio de participação do indivíduo; e
(viii) princípio de responsabilização.

Coletivamente, esses oito princípios são conhecidos como "Fair Information Practice Principles" ou FIPPs.[2] Não por acaso, com uma ou outra alteração ou adaptação, todos esses princípios foram contemplados no artigo 4º, do presente Projeto de Lei do Senado nº 330, de 2013.

Embora o indivíduo ainda tenha (e continuará tendo) papel fundamental na proteção dos dados que dizem respeito a ele e, consequentemente, de sua privacidade, nos cenários de negócio e tecnológico atuais, faz-se necessária a redefinição de responsabilidades. Se não a redefinição, pelo menos seu reajuste em alguma medida.

Instrumento principal da autodeterminação informativa, e símbolo do papel de protagonista do indivíduo na proteção de seus dados, o **consentimento do titular dos dados** é, dentre os meios de legitimação da utilização de dados, o mais evidente e tradicionalmente empregado. Entretanto, tê-lo como pilar principal de legitimação pode não fazer tanto sentido em alguns casos.

[2] OECD, (1980) "OECD Guidelines on the Protection of Privacy and Transborder Data Flows", OECD, Paris.

A complexidade e a diversidade dos usos de dados são inversamente proporcionais à compreensão que os titulares têm das políticas de privacidade que lhes são oferecidas e à seriedade que conferem aos seus repetidos aceites.

Em outras palavras, quanto mais criativos e diversos são usos de dados, menor o entendimento do titular sobre como estão sendo usados, e menor sua disposição em entendê-los, quanto mais se as solicitações forem repetidas (como, de fato, tendem a ser).

Nesse contexto, é natural que, ao receber novas e repetidas solicitações, diminua a compreensão e, até mesmo, a confiança do titular dos dados em quem emite as políticas de privacidade. Como resultado, os consentimentos perdem, em grande medida, seu significado. A esse fenômeno foi atribuída a expressão "fadiga do consentimento".

Se o consentimento e a autodeterminação passam a ter papel menos relevante, qual o caminho a ser trilhado para se garantir usos justos e éticos dos dados pessoais? **A resposta passa pela a inversão de responsabilidades**. O controle de adequação e, por conseguinte, a responsabilidade por esta, deixa de estar centrada no titular dos dados e passa para aquele que fará uso dos mesmos.

É nesse sentido que uma releitura e reposicionamento do princípio da responsabilidade (*accountability* – ou responsabilidade demonstrável) ganhou força entre especialistas sobre o tema. Note que a "**responsabilidade demonstrável**" já fazia parte dos FIPPs (desde 1980) e já consta do artigo 4º, inciso X, deste PLS nº 330/2013. **A mudança foi de ênfase.**

De forma marcante, a responsabilidade demonstrável ganhou força em 2013, ocasião em que a OCDE reviu as Diretrizes (mais de 30 anos depois de sua inauguração) para, dentre outras alterações, incluir o processo de implementação de um "sistema de responsabilidade demonstrável". Em sua essência, a proposta que ora apresentamos é derivada dessa versão revisada das Diretrizes.

Por ***accountability***, ou **responsabilidade demonstrável**, entenda-se, de forma muito resumida, **a criação de um novo papel das empresas e do governo no processo de utilização dos dados**. Será esperado nesse novo sistema ou modelo de proteção que as instituições se responsabilizem, de forma demonstrável, pela utilização e processamento adequados, justos e éticos dos dados pessoais.

Leis de proteção de dados pessoais tem o mandato duplo de, por um lado, proteger de forma robusta os direitos fundamentais à privacidade e à

dignidade humana e, por outro, assegurar o uso criativo de dados em benefício da economia digital e da inovação.

A defesa da responsabilidade demonstrável se dá na medida em que ela não retira do indivíduo o direito de fazer valer seu direito ao controle dos dados que a ele digam respeito. **O que a responsabilidade demonstrável propõe é tirar a responsabilidade primária pela proteção de dados do indivíduo e repassá-la à organização que coleta e faz uso dos dados em seu próprio benefício.**

Esta é a nossa participação no presente debate sobre o tema, na certeza de contar com a atenção dos eminentes pares, em especial do Nobre Relator, Senador Aloysio Nunes Ferreira, para quem solicitamos o indispensável apoio à aprovação da presente emenda.

Sala das Comissões,

Senador ROBERTO ROCHA

(PSB/MA)