Nota da Coalizão Direitos na Rede sobre o Projeto de Lei do Senado nº 330/2013

Proteção de dados pessoais é coisa séria e o texto do Projeto de Lei do Senado nº330/2013 ainda deixa a desejar: não protege devidamente os cidadãos, nem traz segurança jurídica para a economia digital do século XXI no Brasil.

Na última redação apresentada, a legislação não se aplica para atividades de inteligência e repressão de infrações penais, os agentes privados não têm obrigação de apresentar relatório de impacto ou teste de proporcionalidade quando não tiverem o consentimento para o tratamento de dados e se utilizarem de "legítimo interesse" para fazê-lo; as crianças não têm devida proteção especial assegurada, em conformidade com sua fase peculiar de desenvolvimento; tampouco o tratamento dos dados sensíveis, que podem gerar discriminação, foi devidamente regulado, abrindo espaço para usos abusivos.

O PLS 330/13 também falha ao deixar de reconhecer que, no âmbito das relações de consumo, prevalecem as regras de responsabilidade civil estabelecidas pelo Código de Defesa do Consumidor. Além da insegurança jurídica que surgirá de discussões judiciais sobre a relação entre CDC e Lei de Dados Pessoais, o projeto confronta um sistema mais protetivo ao cidadão-consumidor.

E, finalmente, o texto não prevê a criação de uma autoridade de proteção de dados, capaz de garantir sua implementação adequada bem como realizar a regulamentação para sua aderência ao estado de desenvolvimento tecnológico ao longo do tempo e aos novos modelos de negócio.

Soma-se aos problemas de redação do PLS 330/13 uma tramitação problemática e pouco transparente. O texto do relatório a ser votado em regime de urgência no Senado Federal ainda não foi oficializado, o que impede qualquer amadurecimento e mesmo o debate político aberto e saudável. A possibilidade de o Senado votar um tema de tamanha importância, com implicações globais, sem o menor conhecimento prévio do teor da proposta fere o princípio democrático e abre espaço para que os parlamentares incorram no erro em matéria tão relevante.

A Coalizão Direitos na Rede reforça, então, seu apoio ao processo de elaboração de uma Lei de Dados Pessoais em curso na Câmara dos Deputados, resultado de aprofundado debate entre os diferentes setores interessados, que tem redação madura tanto para a garantia de direitos quanto para a segurança jurídica na proteção de dados pessoais, justamente porque construída pela negociação entre governo, sociedade civil e agentes privados.

A opacidade no processo de elaboração da versão final do PLS nº 330/2013 no Senado, elaborado nos últimos dias, macula a imagem de um projeto de lei democrático e construído com a validação de diferentes partes interessadas. A Coalizão Direitos na Rede atenta, assim, para os seguintes pontos do relatório Projeto de Lei de Dados Pessoais que merecem atenção dos Senadores e cidadãos brasileiros.

Pontos problemáticos do Relatório do PLS 330/13

a) Exceções ao poder público
Após várias críticas, o relator alterou o texto, mas o poder público segue excepcionado em pontos preocupantes, como o direito do titular de se opor ao tratamento de dados (art. 18, §3º) e o direito ao cancelamento após o prazo necessário para o tratamento específico. Um artigo da lei também excepciona o poder público de respeitar os princípios e normas da lei sobre transparência e em casos de investigação de improbidade administrativa, situação em que não se justifica exceção equivalente à dada em casos de soberania e segurança nacional.

Nos últimos dias, circulou a informação de que o Ministério Público Federal também estaria pressionando o governo federal e o relator para incluir uma previsão no texto de que, via ato administrativo, seria possível ao poder público limitar ainda mais os direitos do titular em casos de segurança pública ou investigação para repressão de crimes, dando carta aberta para o uso indiscriminado dos dados pessoais dos cidadãos/ãs. Num contexto de vigilância e autoritarismo crescente no país, a medida é extremamente perigosa.

O substitutivo do Senador Ferraço amplia o rol de exceções da lei de dados pessoais. Anteriormente, a lei não se aplicava para tratamento de dados pessoais para fins de segurança pública e segurança nacional. Agora, o projeto afirma que a lei não se aplica para coleta de dados para fins de repressão, investigação de infrações penais e atividades de inteligência (Art, 2º, § 5º).

b) Legítimo interesse
Apesar de determinar que o legítimo interesse só possa ser alegado em situação concreta e necessária, o relatório não traz a previsão de apresentação obrigatória de relatório de impacto nem de teste de proporcionalidade, dando um cheque em branco para as empresas tratarem dados sem consentimento. Hoje, segundo as próprias empresas de tecnologia, o legítimo interesse corresponde à base legal para 80% dos tratamentos de dado em curso hoje no mundo. É fundamental, portanto, que tal hipótese seja mais restrita do que a apresentada no relatório do senador Ferraço.

A redação do substitutivo do Sen. Ferraço possui dois problemas fundamentais. Primeiro, com relação à ausência de amarração do legítimo interesse com os "relatórios de impacto à proteção de dados pessoais" (RIDPD). Não há menção aos RIPDP e não há obrigações jurídicas a serem seguidas pelos responsáveis quando coletam dados sem consentimento, valendo-se do legítimo interesse.

Segundo, há uma ampliação confusa das hipóteses em que "é necessário coletar dados", afirmando-se em lei que é razoável coletar dados pessoais sem consentimento para "inteligência corporativa" (art. 11, §1º, I). Não há nada semelhante em legislações internacionais, além de "inteligência corporativa" ser uma expressão sem enquadramento jurídico, que pode ser interpretada de forma ampla em situações futuras, fazendo com que as coletas de dados pessoais ocorram sem consentimento e sem documentação por meio de análise de impacto à proteção de dados pessoais.

c) Anonimização ao invés de encerramento
O relatório final do Senador Ferraço propõe substitutivo com artigo que prevê que "o encerramento [do tratamento de dados pessoais] implica ou cancelamento ou anonimização dos dados pessoais do titular" (art. 16). A inclusão de um parágrafo que prevê a possibilidade de “anonimização” no lugar de cancelamento implica em uma completa fragilização do direito de oposição e cancelamento de uso de dados pessoais. No limite, um consumidor não poderá nunca efetivar seu direito de cancelamento de uso de dados pessoais, pois o responsável poderá sempre utilizar o trunfo da “anonimização” para manutenção do dado pessoal em suas bases.

d) Dados sensíveis e de crianças
Dados pessoais sensíveis são aqueles passíveis de uso para diferentes formas de discriminação, daí a importância em restringir seu tratamento a situações estritamente necessárias. Apesar de trazer uma definição para o tema, o relatório do senador Ferraço apresenta regulação insuficiente de proteção e restrição adicional ao tratamento desses dados.

No caso de dados de crianças, apesar de o relatório incorporar a necessidade de consentimento parental para o tratamento, a nova redação ignora o direito da criança à informação e a consequente necessidade de o controlador e processador de dados disponibilizarem informações claras e acessíveis sobre o tratamento, observando a condição peculiar de desenvolvimento das crianças, quando o serviço for direcionado a elas ou majoritariamente utilizado por elas. Ao liberar o uso de dados de crianças e adolescentes para fins econômicos, publicidade e marketing, o texto ignora as características peculiares deste grupo, incapaz de analisar o impacto de longo prazo do tratamento de dados e a complexidade de agentes privados envolvidos na cadeia de negócios, e se coloca em oposição do que estabelece a legislação internacional, ao validar a exploração comercial de crianças.

e) Relatório de impacto
Apesar de ser mencionado no texto, não há nenhum artigo ou capítulo que sistematize que elementos devem compor o relatório de impacto e a aplicação desse instrumento de regulação. Em algumas situações específicas, é fundamental prever a obrigatriedade de relatório de impacto prévio ao tratamento de dados pessoais, tais como:
- casos de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais;
- quando for traçar perfil comportamental;
- quando houver tratamento de dados sensíveis;
- quando houver uso compartilhado de dados.

Essa proposta está alinhada com o novo Regulamento Europeu de Proteção de Dados Pessoais, o qual dispõe de um capítulo próprio sobre relatório de impacto à proteção de dados pessoais.

Além disso, é um instrumento essencial e em consonância com a inovação do relatório de senador Ricardo Ferraço sobre governança em privacidade. Ora, para que existam boas práticas e programas corporativos em privacidade é pré-condição que haja o mapeamento, gerenciamento e mitigação dos ricos das atividades de tratamento de dados, o que só pode

ser alcançado por meios desses relatórios de impacto. Essa é a grande virada e novidade no campo da proteção de dados pessoais. Sem esse capítulo de sistematização, nós corremos o risco da nossa futura lei já nascerá "velha".

f) Responsabilidade civil
O texto não traz a previsão de que, no âmbito das relações de consumo, prevalecem as regras de responsabilidade civil estabelecidas pelo Código de Defesa do Consumidor. O texto deixava para o juiz definir qual lei deve prevalecer em casos de violação de direitos. Na versão do relatório do Senador Ferraço, o art. 36 prevê um regime de responsabilização dos controladores e operadores, permitindo que responsáveis subcontratem operadores, que deverão seguir instruções contratuais de atuação.

O artigo 37 prevê isenções de responsabilidade para "aqueles que tiverem acesso aos dados pessoais". A Coalizão Direitos na Rede recomenda redação adotada no Projeto de Lei nº 5276/16, com a inclusão de artigo que mencione expressamente que "as hipóteses de violação ao direito do titular no âmbito das relações de consumo permanecem inteiramente sujeitas às regras de responsabilidade previstas na Lei 8.078, de 11 de setembro de 1990, observado o inciso III do art. 4º daquela lei".

Desse modo, garante-se um sistema de responsabilidade subjetiva para hipóteses em que não há relações de consumo e um sistema de responsabilidade objetiva, nos moldes do Código de Defesa do Consumidor, quando houver identificação clara de relação de consumo.

g) Sanções
As multas previstas no relatório tem como teto 2% do faturamento da empresa ou do grupo econômico, destoando do padrão internacional de 4%.

h) Autoridade de proteção de dados pessoais
A experiência internacional demonstra que a efetividade de uma lei geral de proteção de dados requer uma autoridade garantidora capaz de oferecer segurança jurídica para os setores público e privado. Tal autoridade teria a atribuição de aconselhar, editar normas cogentes e fiscalizar a observância das regras legais, bem como aplicar as sanções quando da violação. Para a constituição de seus executivos, é preciso garantir o princípio constitucional da pluralidade, mediante composição multissetorial. A entidade reguladora também deve ser financeiramente independente, com dotação orçamentária própria, que permita autonomia funcional e formação de quadros competentes e qualificados.

Diante da competência constitucional exclusiva do Poder Executivo para propor projetos de lei que criem órgãos, entendemos que o PLS não poderia propor a existência de uma Autoridade Brasileira de Proteção de Dados Pessoais. Este, porém, é um ponto crucial para qualquer Lei de Proteção de Dados Pessoais.