CONSULTORIA LEGISLATIVA

COMENTÁRIOS AO PL 5276/16, QUE DISPÕE SOBRE O TRATAMENTO DE DADOS PESSOAIS

Claudio Nazareno
Consultor Legislativo da Área XIV
Ciência e Tecnologia,
Comunicações e Informática

NOTA TÉCNICA

JUNHO/2016

CÂMARA DOS DEPUTADOS

SUMÁRIO

I – INTRODUÇÃO

A discussão sobre proteção ao tratamento de dados é extremamente relevante em momentos em que governos e corporações privadas adquirem enormes quantidades de dados a respeito de pessoas, estando estas na condição de consumidores, pacientes, usuários ou cidadãos. A máxima “dados são o novo petróleo” é repetida em reuniões de negócios, ao ponto de a análise de dados e a identificação de novas oportunidades representar uma fronteira significativa no setor de serviços. Apenas para ilustrar essa afirmação, a Microsoft, ao adquirir a Linkedin, em 2016, pagou 26 bilhões de dólares por uma empresa que possui um cadastro profissional de 430 milhões de usuários e 100 milhões de visitantes por mês (The Economist, 2016). O valor representa 60 dólares por usuário ou 260 dólares por visitante mensal. O Facebook, que possui 1 bilhão de usuários ativos diários (e 1,6 bilhão mensais), fatura mais de 5 bilhões por trimestre (Facebook, 2016). Em outras palavras, cada usuário ativo diário que se utiliza do aplicativo, quer seja postando ou curtindo conteúdos, representa 20 dólares de faturamento anual para a empresa.

No Brasil a importância dos dados não é diferente. Em 2013, foi divulgada a existência de convênio entre o Serasa e o Tribunal Superior Eleitoral permitindo o acesso ao cadastro eleitoral. Com a polêmica veio a público a informação de que esse tipo de acordo não era novidade em outras instâncias do judiciário (Rover, 2013).

Porém, mais do que apenas acordos comerciais, a exploração de dados pessoais tornou-se programa de Estado, como evidenciado no *caso Snowden* (ver Rocha, 2015), em diversos países, com o desenvolvimento de procedimentos de coletas de dados que ultrapassam fronteiras.

Nesse contexto, ocorrem movimentos pelo mundo demandando maior proteção aos dados pessoais que, pode-se dizer, culminaram com a Resolução da ONU, de 25 de novembro de 2013, sobre "Direito à Privacidade na Era Digital”. O Projeto de Lei (PL) 5276, ora em análise, surge a partir desta situação.

No caso brasileiro, a proposta de regulamentação também pode ser considerada um complemento aos ditames estabelecidos pelo Marco Civil da Internet (Lei no 12.965/14). Enquanto o Marco transpôs para o mundo virtual garantias constitucionais, como de liberdade de expressão e de informação, o PL dá disposições mais específicas quanto à forma como dados pessoais coletados podem ser tratados, armazenados e dispostos, tanto por entidades públicas quanto privadas. Ademais, convêm ressaltar que o escopo das disposições do projeto ora em análise ultrapassa o mundo virtual. Caso aprovada, a regulamentação será aplicada no tratamento de dados em qualquer meio, não apenas na internet.

Conforme Mensagem da Presidência da República, esta proposta do Poder Executivo foi submetida a processo de consulta pública junto ao Ministério da Justiça, sendo as contribuições consolidadas em parceria com o Nic.br, vinculado ao CGI.br, e a Winweb, da Universidade Federal de Minas Gerais. A Mensagem também ressalta que a proposta é fruto da citada resolução da ONU e que "109 países possuem normas nesse sentido e mais de 90 destes têm uma autoridade pública específica especializada no tema."

Devido à complexidade do assunto, o PL possui 56 artigos, divididos em nove capítulos. Esta Nota Descritiva se concentrará nos aspectos mais relevantes que, consequentemente, poderão suscitar maiores debates. Tratam-se das disposições que dizem respeito à definição de dados sensíveis, à transferência (repasse e venda) de dados pessoais entre empresas, às informações financeiras e de crédito, a crianças e adolescentes e quanto à criação de autoridade específica para a proteção de dados.

As discussões serão contextualizadas com exemplos estrangeiros.

II – DADOS SENSÍVEIS

Art. 5º, III (do PL) - dados sensíveis: dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a

sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos;

Para o tratamento de dados sensíveis, o projeto determina a necessidade de haver "consentimento livre, inequívoco, informado, expresso e específico pelo titular" (Art. 11). Já para os demais dados, o consentimento deverá ser "livre, informado e inequívoco" (Art. 7o).

A definição de dados sensíveis no PL guarda forte sintonia com a Convenção do Conselho da Europa no 108, "Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automático de Dados Pessoais", que determina, no artigo 6o:

> "Dados pessoais que revelem a origem racial, opiniões políticas, religiosas ou de outras crenças, bem como dados relativos à saúde pessoal ou à vida sexual não podem ser processados automaticamente ao menos que leis nacionais estabeleçam garantias adequadas. O mesmo se aplica a dados pessoais relativos a condenações criminais."

Também guarda semelhança com o que prescreve a Diretiva Europeia no 46, de 1995, conhecida como Diretiva de Proteção de Dados, que estabelece no artigo 8:

> "1. Os Estados-membros proibirão o tratamento de dados que revelem a origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual.
>
> 2. O parágrafo 1 não se aplica quando:
>
> (a) o titular dos dados deu consentimento explícito ao tratamento desses dados, salvo se a legislação do Estado-Membro estabelecer que a proibição referida no parágrafo 1 não pode ser retirada por consentimento da pessoa em causa; ou...."

Em que pese o PL especificar a necessidade do consentimento, há outras condições em que dados pessoais poderão sofrer tratamento. O mesmo artigo 11 permite o tratamento de dados sensíveis em vários casos, mesmo sem consentimento, ainda que não seja possível garantir sua anonimização, como em casos de pesquisas comerciais.

É importante ressaltar também que, ao contrário da regulamentação europeia, os dados de condenações criminais (ou registros policiais) não são considerados sensíveis.

III – TRANSFERÊNCIA NACIONAL E INTERCONEXÃO DE DADOS

O projeto não oferece salvaguardas específicas para a transferência nacional ou interconexão de dados entre entidades privadas (ou para fins comerciais). Ademais, a proposta não requer consentimento para essas transações. Assim, clientes/usuários/consumidores de determinadas empresas podem ter seus dados comercializados/repassados entre empresas privadas sem consentimento expresso para tal.

IV – INFORMAÇÕES DE PERFIL, FINANCEIRAS E DE CRÉDITO

A Diretiva Europeia estabelece que dados referentes a perfis pessoais não podem sujeitar o titular dos dados a decisões oriundas exclusivamente de tratamento automatizado. Entre os aspectos pessoais encontram-se performance no trabalho, perfil de crédito, confiança, conduta, etc (art. 15.1). Disposição similar, porém genérica, encontra-se no PL (art. 20).

Já o Código dos Estados Unidos estabelece que informações de entidades financeiras não podem ser repassadas sem consentimento expresso, o chamado “opt out” (US Code § 6802).

VI – TRATAMENTO DE DADOS DE CRIANÇAS E ADOLESCENTES

O PL dispõe de um comando genérico determinando que o "tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado no seu melhor interesse, nos termos da legislação pertinente" (Art. 14).

Nos EUA, a Lei COPPA (Children's Online Privacy Protection Act, de 1998, constante no Código Americano Título 15, Capítulo 91, §§6501–6506), que trata da proteção de dados pessoais das crianças na internet, determina como regra geral ser ilegal a coleta de dados de crianças (abaixo de 13 anos de idade) sem o consentimento dos país. A Lei daquele país excetua alguns poucos casos, como quando os dados não serão armazenados ou serão utilizados uma única vez.

VI – AUTORIDADE ESPECÍFICA PARA A PROTEÇÃO DE DADOS

A existência de autoridade específica a cargo da proteção de dados pessoais varia entre os países. O Reino Unido possui o ICO (Information Commissioner's Office), estabelecido na forma de agência reguladora ligada ao Ministério afeito às comunicações (Department for Media, Culture and Sport). O ICO possui Presidente, Vice e quatro Diretores. A França possui a Comissão Nacional da Informática e das Liberdades (CNIL - Commission Nationale de l'Informatique et des Libertés), com a função de proteção dos dados das pessoas. A Comissão é uma autoridade independente, composta por 17 membros (2 deputados; 2 senadores; 2 do Conselho Francês afeito às áreas econômica, social e do meio ambiente; 2 do Executivo; 2 da Suprema Corte; 2 da Corte de Contas; 5 figuras públicas – das quais uma é indicada pelo Senado, outra pela Câmara e três pelo Executivo).

Nos EUA, a proteção de dados não possui lei específica, sendo compartilhada entre várias autoridades. Como regra geral, a privacidade é tratada como um aspecto de proteção aos consumidores e, portanto, está sob a égide da FTC (Federal Trade Commission – Comissão Americana de Comércio). Entretanto, dados sobre saúde, por exemplo, estão a cargo do Departamento da Saúde e Serviços Humanos (U.S. Department of Health & Human Services) e sob a tutela da Lei que

trata da portabilidade de planos de saúde (Health Insurance Portability and Accountability Act (HIPAA) (42 U.S.C. §1301 et seq.)).

Para o caso brasileiro, o PL prevê um órgão de fiscalização e um Conselho Nacional com poder consultivo e de avaliação. A proposta estabelece que o Conselho deverá ser formado por 15 membros, indicados pelo Ministério da Justiça, segundo os seguintes critérios: 7 representantes do Poder Executivo, 1 do Congresso Nacional, 1 do CNJ, 1 do Ministério Público, 1 do CGI, 1 da sociedade civil, 1 da academia e 2 do setor privado.

VII – CONSIDERAÇÕES FINAIS

O Projeto de Lei inova na proteção aos dados pessoais e estabelece uma série de salvaguardas com o intuito de proteger a intimidade, a privacidade e o desenvolvimento da personalidade das pessoas, de ações de coleta e tratamento de dados por parte de governos e entidades privadas.

A proposta pode ser considerada um complemento ao recente Marco Civil da Internet, que transpôs para o mundo virtual as garantias constitucionais e estabeleceu princípios, direitos e deveres para o uso da internet no País.

A proposta guarda sintonia com o estado atual do mundo, em que informação tem ganhado importância estratégica e comercial. O projeto é extremamente detalhado nas atividades que concernem a esfera pública, prevendo que o tratamento de dados por parte da Administração deverá seguir estritos ditames, além de garantir aos cidadãos ampla informação sobre os dados coletados. Por outro lado, o projeto permite a exploração de dados pessoais, pelo mercado, de maneira bastante flexível, facilitando a geração de negócios a partir desse insumo.

Entretanto, as disposições **poderão suscitar, na visão de seus críticos, as seguintes considerações:**

1) A não inclusão de dados criminais e judiciais no rol de dados sensíveis encontra-se em desacordo com outros padrões internacionais.

2) Ao contrário da transferência internacional de dados, não há parte específica no texto dedicada à transferência ou à interconexão nacional de dados por entes privados, o que permite, por exemplo, a comercialização de dados pessoais com terceiros sem o consentimento expresso do titular.

3) O artigo que trata de dados de crianças e adolescentes é impreciso quanto aos objetivos, garantias e possibilidades acerca do tratamento das informações desses vulneráveis. A legislação americana é muito mais rígida no quesito.

4) Dados acerca do perfil de crédito e de consumo não possuem provisões específicas, como ocorre em outros países.

5) Embate entre criação de órgão específico ou atribuição da atividade a outro já existente, para a tutela das práticas de tratamento de dados, assim como a composição e as atribuições do conselho auxiliar proposto.

VIII – REFERÊNCIAS

FACEBOOK. Facebook Q1 2016 Results, 2016. Disponível em: <https://s21.q4cdn.com/399680738/files/doc_financials/2016/FB_Q116_Earnings_Slides.pdf>. Acesso em: 17 jun. 2016

ROCHA, F. Espionagem e Internet. Caderno Aslegis, v. 49, 2015.

ROVER, T. Acordos com Serasa são frequentemente contestados. Disponível em: <http://www.conjur.com.br/2013-ago-08/acordos-tribunais-serasa-sao-frequentemente-contestados-justica>. Acesso em: 17 jun. 2016.

THE ECONOMIST. LinkedUp. Disponível em: <http://www.economist.com/news/business-and-finance/21700605-it-one-most-expensive-tech-deals-history-it-may-not-be-smartest-making-sense>. Acesso em: 17 jun. 2016.