O novo anteprojeto de proteção de dados pessoais e as startups e provedores de serviços na Internet

A nova redação do anteprojeto de proteção de dados pessoais foi apresentada em novembro de 2015 e tende a se transformar em Projeto de Lei de autoria do Poder Executivo Federal. Muito em breve, teremos um projeto que tende a se tornar a primeira lei infraconstitucional a dispor sobre o tratamento dos dados pessoais. Teremos ainda a criação de um Conselho Nacional de Proteção de Dados Pessoais, denominado na lei de "órgão competente", que coordenará e fiscalizará todas estas questões no País, incluindo a criação de políticas sobre o tema.

A norma em estudo disciplina o tratamento de dados realizados por pessoas físicas e jurídicas, com o objetivo de proteger os direitos fundamentais, o livre desenvolvimento da personalidade e a privacidade das pessoas. Se aplica a todas as pessoas jurídicas que tratem dados, pouco importando o local da sede ou o local do armazenamento dos dados, desde que a operação de tratamento seja realizada no território nacional, os dados pessoais tenham sido coletados no Brasil ou a atividade de tratamento tenha por escopo a oferta de bens e serviços no território nacional. Aplicações estrangeira que ofereçam serviços no Brasil não devem desconsiderar a norma.

A grande celeuma se situava em saber o que se entendia por "dados coletados em território nacional". A versão atual do APL traz uma solução, onde seriam considerados dados coletados em território nacional as hipóteses em que o titular dos dados estiver de fato neste território

Ficam fora da legislação o tratamento dos dados realizados com

fins jornalísticos, artísticos, acadêmicos, para fins pessoais ou realizados para fins de segurança pública e investigação. Ou seja, atividades de inteligência cibernética estariam fora do escopo da norma, desde que realizadas por pessoas de direito público, embora seja tema a ser regulamentado por lei. Já a atividade de pesquisa poderá ser realizada com dados pessoais, desde que haja a anonimização sempre que possível

Em seu artigo quinto o anteprojeto define o que seriam os "dados pessoais", dados relacionados a pessoa natural identificada ou identificável, informando que também se enquadram neste contexto os "identificadores eletrônicos" quando estes estiverem relacionados a uma pessoa (índices, códigos únicos, coordenadas, etc). Já "dados sensíveis" seriam os dados pessoais de maior criticidade ou cuja proteção deva ser ainda maior, como preferência sexual, política, religiosa, dados genéticos e biométricos, etc.

É muito comum que startups de aplicações web utilizem e tratem dados pessoais. Toda a atividade de tratamento de dados deve respeitar os princípios previstos na norma, dentre os quais, o da finalidade, onde o tratamento deve ser realizado para finalidades legítimas, específicas e informadas ao titular.

O tratamento de dados pessoais só pode ocorrer pelo consentimento livre e inequívoco do titular ou por obrigação legal. Também é previsão da norma a possibilidade de o titular, a qualquer tempo, solicitar informações sobre o tratamento de seus dados.

Para empresas de Internet, dados e para o mercado de aplicativos e serviços web fica o alerta: Sempre que a coleta de dados for condição para instalação ou uso do serviço, o usuário deverá ser informado deste fato e dos meios que terá para controlar o tratamento dos seus dados. Lembrando que o consentimento não precisa ser por escrito e considerando a era da Internet, poderá se dar por "outro meio que o certifique". Assim, um "aceitar" para prosseguir na aplicação ou serviço,

devidamente registrado, terá sua validade.

As empesas de serviços web deverão investir nesta estrutura pois pelo APL, o ônus é delas em provar que o usuário consentiu com o tratamento de seus dados. Um canal para que o usuário possa revogar seu consentimento também demonstra-se boa prática. A revogação deverá se dar por manifestação expressa.

Já quando diz respeito a dados pessoais sensíveis o anteprojeto confere outro tratamento. O consentimento, para dados pessoais sensíveis (religião, preferência sexual, etc.), deve ser expresso e apartado do consentimento para tratamento de outros dados pessoais. Ainda, o titular não poderá ser penalizado, preterido ou discriminado pelo tratamento dos dados pessoais sensíveis. No que tange a "dados anonimizados" ou dados dissociados do seu titular, o APL prevê que estes podem ser considerados dados pessoais para fins de proteção da norma, desde que o processo seja revertido ou possa ser revertido. Cada caso deverá ser analisado

Do mesmo modo, poderão ser considerados dados pessoais os dados utilizados para formação de perfis de pessoas, mesmo que não identificadas. Assim, o tratamento de dados "públicos" em uma timeline, por exemplo, mas que revelem perfis, condutas privadas, comportamentos e opções sensíveis, pelo APL, pode elevar os dados tratados ao grau de dados pessoais.

Os padrões de anonimização poderão ser debatidos por órgão competente.

Destaca-se que o titular dos dados tem vários direitos assegurados pela norma, como o de descobrir se teve dados tratados e até mesmo acessar tais dados, podendo requerer a correção, bloqueio, anonimização ou eliminação de dados desnecessários, excessivos ou contrários a Lei. No que cabível, à tutela de proteção aos dados pessoais, aplica-se o Código de Defesa do Consumidor. Os direitos acima serão

exercidos por meio de requerimento, que deverá ser respondido pelo responsável pelo tratamento dos dados na startup. As informações requeridas pelo titular poderão ser fornecidas por meio eletrônico.

As defesas dos titulares de dados poderão ser exercidas em juízo coletivamente, por institutos e associações, nos moldes dos arts. 81 e 82 do Código de Defesa do Consumidor e demais instrumentos.

Para o Poder Público, aplicam-se as mesmas regras que aplicável às empresas, devendo este indicar um responsável pelo tratamento de dados. É vedado ao Poder Público transferir dados pessoais a entidades privadas com exceção para casos de execução descentralizada de atividade pública, informando-se o órgão competente de fiscalização.

O Anteprojeto de Lei também regulamenta a transferência internacional de dados, assegurando que só será permitido o envio de dados a países que assegurem nível de proteção a dados pessoais equiparáveis.

Este órgão competente, que será criado a partir da vigência da norma, também avaliará pedidos de permissão para transferência internacional de dados de grandes provedores de serviços web, que poderão submeter suas normas corporativas globais para aprovação. Nas transferências de dados, tanto cedente como cessionário respondem solidária e objetivamente por danos causados no tratamento dos dados.

A Lei também obriga às empresas a definirem um “encarregado pelo tratamento de dados pessoais”, pessoa indicada para mediar as reclamações de titulares, receber comunicações do órgão competente, adotar providências, prestar esclarecimentos e orientar a empresa e colaboradores nas melhores práticas de privacidade, o que no exterior se denomina “Privacy Officer”.

No que tange à responsabilidade civil o APL é claro em seu artigo 42. Todo aquele que, no exercício do tratamento de

dados pessoais, causar dano patrimonial ou moral, deverá repará-lo. No que diz respeito a invasões a sites, aplicativos web e vazamento de dados, a norma é intensa ao disciplinar que o operador deve adotar medidas de segurança aptas a proteger os dados pessoais. Quem definirá padrões será o órgão competente a ser criado no âmbito da Legislação. Porém é fato que uma consultoria de segurança e privacidade deverá ser acionada para avaliar o ambiente do empresário e possíveis brechas em seu negócio digital. Aliás, até os sistemas de tratamento de dados pessoais já deverão ser estruturados com requisitos de segurança. Políticas e boas práticas serão estimuladas nas empresas e startups.

De se destacar que os ataques ou incidentes a um serviço web ou móvel deverão ser comunicados pela empresa ao órgão competente em tempo razoável, com a descrição de todos os detalhes como informações envolvidas e riscos. Daí a necessidade de um Privacy Officer, que centralizará e coordenará todas estas ações na empresa.

Por fim, aquele que violar a legislação poderá, sem prejuízo de outras sanções civis e criminais, sofrer sanções administrativas, elencadas no art. 52, que pode ser multa, suspensão para operação de tratamento de dados pessoais, dentre outras.