Brasília, 02 de junho de 2017.

Contribuições acerca dos pontos a serem abordados na Lei de Tratamento e Proteção de Dados Pessoais

Ref.: Solicitação da Exma. Sra. Deputada Federal Bruna Furlan.

DADOS PESSOAIS E A DEFESA DO CONSUMIDOR

Os dados pessoais dos consumidores sempre foram atraentes para o mercado, tendo em vista que a informação pessoal fomenta uma maior capacidade de organizar um planejamento de produtos e vendas mais eficiente, favorecendo a criação de mecanismos de atração pelo mercado, bem como publicidades voltadas às reais características dos consumidores. A abundância de informação passível de ser obtida sobre o consumidor amplia sua vulnerabilidade em detrimento daqueles que detém as informações pessoais.

Uma lei sobre a proteção dos dados pessoais permite que o cidadão tenha o controle de como suas informações serão utilizadas por organizações, empresas e pelo governo. Ela deve estabelecer padrões mínimos a serem seguidos, como: a vinculação do uso das informações pessoais à finalidade específica para a qual deverão ser utilizados, bem como a criação de um ambiente seguro e controlado, definição de seu âmbito de atuação, regras sobre as modalidades de tratamento de dados pessoais, os princípios a serem seguidos, responsabilidade dos agentes, entre outras peculiaridades.

O impacto de norma deste gênero é relevante no sentido de diminuir a assimetria informacional e a situação de vulnerabilidade do consumidor em relação àquela que utiliza e compartilha desses dados. Ademais, a lei sobre proteção de dados pessoais apresenta conteúdo de elevada tecnicidade ao definir novos conceitos e portar inovações à ordem jurídica, de modo que se torna necessário o amadurecimento do tema nos diversos setores da sociedade.

Nesse tocante, sobreleva mencionar que a Secretaria Nacional do Consumidor juntamente com a Secretaria de Assuntos Legislativos, ambas do Ministério da Justiça, promoveram debates públicos sobre o Anteprojeto de Lei de Tratamento de Dados Pessoais no escopo obter elementos à sociedade no sentido de formular uma proposta normativa sobre proteção de dados pessoais capaz de garantir e proteger a dignidade e os direitos fundamentais da pessoa, particularmente em relação à sua liberdade, igualdade e privacidade pessoal e familiar.

Portanto, relevante se torna a interlocução dos órgãos envolvidos, de modo que a Senacon deseja contribuir à realização de um texto final capaz de atender os anseios da sociedade. A defesa do consumidor está incumbida de proporcionar respostas aos possíveis riscos ligados ao tratamento da informações pessoais dos consumidores, de modo a proporcionar tanto a proteção contra utilização abusivas de suas informações como garantias de que suas escolhas sobre a utilização de seus próprios dados sejam livres e transparentes.

A PROTEÇÃO DE DADOS COMO DIREITO FUNDAMENTAL

No ordenamento jurídico brasileiro o reconhecimento da proteção de dados como um direito autônomo e fundamental não se encontra explícito, contudo recebe o alicerce das garantias constitucionais, expressas na Constituição Federal, de igualdade, liberdade e dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada.

Em relação à estrutura normativa que geralmente apresentam as normativas de proteção de dados, é oportuno mencionar que alguns princípios de proteção de dados pessoais perpassam praticamente a totalidade das cerca de 109 leis gerais de proteção de dados pessoais hoje existentes. Em uma síntese de natureza generalista, estes princípios são:

(i) Princípio da transparência, pelo qual o tratamento de dados pessoais não pode ser realizado sem o conhecimento do titular dos dados, que deve ser informado especificamente sobre todas as informações relevantes concernentes a este tratamento;

(ii) Princípio da qualidade, pelo qual os dados armazenados devem ser fieis à realidade, atualizados, completos e relevantes, o que compreende a necessidade de que sua coleta e seu tratamento sejam feitos com cuidado e correção, e de que sejam realizadas atualizações periódicas conforme a necessidade;

(iii) Princípio da finalidade, pelo qual qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta. Este princípio possui grande relevância prática: com base nele se fundamenta a restrição da transferência de dados pessoais a terceiros, além do que se pode, a partir dele, estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade (fora da qual haveria abusividade);

(iv) Princípio do livre acesso, pelo qual o indivíduo deve ter acesso às suas informações armazenadas em um banco de dados, podendo obter cópias destes registros; após este acesso e de acordo com o princípio da qualidade, as informações incorretas poderão ser corrigidas, aquelas registradas indevidamente poderão ser canceladas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou mesmo pode-se proceder a eventuais acréscimos;

(v) Princípio da segurança física e lógica, pelo qual os dados devem ser protegidos por meios técnicos e administrativos adequados contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado.

Verifica-se, com o breve apanhado protetivo, que a tutela autônoma dos dados pessoais é considerado um direito fundamental, inclusive já consagrado em outros Países, consoante os termos da Convenção nº 108 do Conselho da Europa, que discorre:

Considerando que a finalidade do Conselho da Europa é conseguir uma união mais estreita entre os seus membros, nomeadamente no respeito pela supremacia do direito, bem como dos direitos do homem e das liberdades fundamentais;

Considerando desejável alargar a proteção dos direitos e das liberdades fundamentais de todas as pessoas, nomeadamente o direito ao respeito pela vida privada,

tendo em consideração o fluxo crescente, através das fronteiras, de dados de carácter pessoal susceptíveis de tratamento automatizado**;**

Reafirmando ao mesmo tempo o seu empenhamento a favor da liberdade de informação sem limite de fronteiras;

Reconhecendo a necessidade de conciliar os valores fundamentais do respeito pela vida privada e da livre circulação de informação entre os povos, acordaram o seguinte:

Artigo 1º - Objectivos e finalidades

A presente Convenção destina-se a garantir, no território de cada Parte, a todas as pessoas singulares, **seja qual for a sua nacionalidade ou residência, o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito («protecção dos dados»).**

Nesta senda, a definição de dados pessoais, disposta no art. 2º da Convenção nº 108 aponta para: "*qualquer informação relativa a uma pessoa singular identificada ou susceptível de identificação («titular dos dados»)"*, sendo portanto estes os titulares e detentores da proteção fundamental, que ora se propõe regulamentar.

A Senacon entende que a técnica de caracterização dos dados anônimos é oportuna porém observa a necessidade de que as exceções da aplicações da lei para estes não acabe por proporcionar a criação de uma espécie de “ponto cego” no qual dados que possam influir diretamente sobre a vida do cidadão não acabem fora do âmbito de aplicação da lei, sugere, para assegurar a sua efetividade, a inclusão de mais dois instrumentos: (i) previsão de que a lei se aplicará, ainda que os dados sejam anônimos, quando organizados de forma a corresponder ao perfil de uma pessoa, ainda que não identificada (necessário no caso também definir “perfil”); (ii) prever a proibição expressa do recurso à de-anonimização.

Ainda no que tange às definições, a Senacon sugere a introdução da figura do "encarregado" que é a pessoa natural, indicada pelo responsável, que atua como canal de comunicação perante os titulares e o órgão competente, este deve funcionar como o ponto focal. O encarregado (que pode ser uma pessoa que acumule outras funções dentro de uma estrutura organizacional) serve como ponto focal dentro em uma organização para os temas relacionados à proteção de dados bem como proporciona a terceiros (clientes, consumidores e titulares de dados com interesse justificado) um canal de contato para o encaminhamento de dúvidas e eventuais demandas.

DOS DIREITOS BÁSICOS DOS TITULARES

Proporcionar ao cidadão controle sobre o que é feito com os seus dados pessoais é a finalidade da norma, de forma que possa livremente decidir sobre a coleta, armazenamento e tratamento de seus dados pessoais.

DO TRATAMENTO DOS DADOS PESSOAIS

A noção de que o armazenamento de dados pessoais pode representar algum tipo de risco ao cidadão, assim como o entendimento de que qualquer tratamento de

dados deva ser justificado, são alguns dos preceitos basilares da proteção aos dados pessoais. A sua obediência busca evitar que dados pessoais sejam tratados de forma indefinida

Dessa forma, a regra geral é de que os dados pessoais sejam cancelados após o esgotamento da finalidade para a qual foram coletados, o que evita uma apropriação indevida dos dados.

Porém, há situações nas quais os interessados no tratamento poderão justificar a manutenção dos dados para além da sua finalidade originária, como para casos de pesquisa histórica. Há igualmente situações que os dados também poderão ser mantidos, contudo sem o anterior vínculo com o seu titular, quando os dados são submetidos a um processo de dissociação.

DA RESPONSABILIZAÇÃO

A lei protege os titulares dos dados pessoais no sentido de coibir abusos e ilegalidades oriundas de práticas cometidas pelos detentores de dados pessoais, sejam eles pessoa jurídica individual ou associações. A Senacon sugere a inclusão de previsões normativas que possam incentivar a adoção de normas deontológicas e de melhores práticas pelos setores e empresas responsáveis pelo tratamento de dados pessoais. O Anteprojeto do Ministério da Justiça traz neste ponto, especificamente em seu art. 48, a seguinte previsão:

Art. 48. Os responsáveis pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas que estabeleçam condições de organização, regime de funcionamento, procedimentos, normas de segurança, padrões técnicos, obrigações específicas para os diversos envolvidos no tratamento, ações formativas ou mecanismos internos de supervisão, observado o disposto nesta Lei e em normas complementares sobre proteção de dados.

Parágrafo único. As regras de boas práticas disponibilizadas publicamente e atualizadas poderão ser reconhecidas e divulgadas pelo órgão competente.

A formulação e adoção de normas deontológicas por órgãos, empresas ou setores do mercado que realizem tratamento de dados pessoais representa tanto um compromisso concreto destes em efetivar melhores práticas no processamento de informações pessoais que respeitem e superem os parâmetros estabelecidos por lei como também facilita a adaptação da normativa às características específicas de cada setor do mercado. Considerando a grande heterogeneidade entre os variados setores que se utilizam de dados pessoais, tal iniciativa facilita a absorção da normativa em setores específicos e diversos, daí o interesse em fomentar este processo.

DA SEGURANÇA E SIGILO DE DADOS

No âmbito do capítulo referente à segurança, na opinião desta Secretaria, são necessárias previsões que procurem contemplar os procedimentos a serem adotados nos casos em que ocorrem incidentes de segurança ou, em terminologia adotada coloquialmente, quando ocorre um "v*azamento de dados*".

Na esteira de normativas presentes nos Estados Unidos, em diversos países europeus e outros, alguns procedimentos que procurem aumentar a transparência e aumentar o cuidado com os titulares dos dados em casos de incidentes de segurança nos quais as suas informações possam ter sido disponibilizadas a terceiros não autorizados podem ser incluídos, de forma a reforçar as garantias dos titulares. Entre estes procedimentos estão a comunicação obrigatória do incidente a um órgão competente para que este decida pela publicização ou não do fato, com eventual notificação a todos os titulares afetados. Outras disposições podem, por exemplo, ajudar a avalizar a extensão dos danos, como a verificação da adoção da criptografia para o armazenamento dos dados.

O Anteprojeto de Lei do Ministério da Justiça apresenta uma proposta de normativa neste sentido que apresentamos abaixo, a título de informação, adiante:

Art. 44. O responsável deverá comunicar imediatamente ao órgão competente a ocorrência de qualquer incidente de segurança que possa acarretar prejuízo aos titulares.

Parágrafo único. A comunicação deverá mencionar, no mínimo:

I - descrição da natureza dos dados pessoais afetados;

II - informações sobre os titulares envolvidos;

III - indicação das medidas de segurança utilizadas para a proteção dos dados, inclusive procedimentos de encriptação;

IV - riscos relacionados ao incidente; e

V - medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos de prejuízo.

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.

§ 1o No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis para terceiros não autorizados a acessá-los.

-

§ 2o A pronta comunicação aos titulares afetados pelo incidente de segurança será obrigatória,

independente de determinação do órgão competente, nos casos em que for possível identificar que o incidente coloque em risco a segurança pessoal dos titulares ou lhes possa causar danos.

Art. 46. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Art. 47. Órgão competente poderá estabelecer normas complementares acerca de critérios e padrões mínimos de segurança, inclusive com base na evolução da tecnologia.

Finalmente, apontamos que o avanço da tecnologia da informação amplia enormemente o potencial de coleta, processamento e utilização de dados pessoais, o que representa, por um lado, uma oportunidade de geração de novos conhecimentos e serviços mas, por outro, pode acarretar graves riscos aos direitos da personalidade do cidadão, ao acesso a serviços e bens, além de uma grande insegurança jurídica para o ambiente de negócios de tecnologia da informação existente no país, bem como para o comércio exterior, por conta da desconformidade da legislação brasileira atual aos padrões internacionais existentes neste tema.

Não é apenas pela defasagem em comparação a outros países que urge a necessidade de promulgação desta norma legal. A utilização, cada vez mais intensa, de dados pessoais na sociedade da informação cria um desequilíbrio entre os poderes dos indivíduos, titulares de seus próprios dados pessoais, e os dos utilizadores de tais dados, justamente pela quantidade de informações pessoais que as novas tecnologias são capazes de agregar e utilizar. Para que esses dados possam ser utilizados com fins transparentes e legítimos, ao mesmo tempo em que sejam garantidos os direitos de seus titulares, são necessárias normas e mecanismos institucionais que estabeleçam os parâmetros e limites deste tratamento, até mesmo no momento de término dessa relação.

Diante do exposto, fica claro que os dados pessoais merecem uma tutela forte e específica do ordenamento jurídico. O processamento dessas informações influencia diretamente a vida das pessoas, afetando oportunidades, escolhas e interações sociais, elementos que compõem o livre desenvolvimento da sua própria personalidade. Tendo isso em vista, é imperativo que haja um conjunto de princípios que norteiem o tratamento desses dados por terceiros, entre os quais podem ser destacados sua utilização somente para finalidades específicas, adequadas e necessárias, além da regra de que o responsável pela coleta desses dados deva mantê-los em segurança, e que não os utilize para discriminação e permita o acesso facilitado ao titular.

O estabelecimento de regras sobre a proteção de dados pessoais possui, portanto, duas funções: proteger o titular dos dados e, ao mesmo tempo, favorecer a sua utilização dentro de um patamar de segurança, transparência e boa-fé. Dessa forma, a utilização lícita de dados será incentivada pela delimitação de um espaço de segurança jurídica, favorecendo o fluxo de dados por agentes responsáveis e o desenvolvimento de setores econômicos ligados, por exemplo, às tecnologias de informação. Nesse sentido, a proposta também trata da transferência internacional de dados e o condicionamento de sua ocorrência para determinadas circunstâncias, entre elas, para países que tenham nível de proteção equiparável ao brasileiro. Essa disposição implica que a partir da promulgação da lei brasileira de proteção de dados pessoais, o país estará apto a entrar no rol de Estados com os quais as empresas europeias podem realizar negócios que envolvam o tratamento de dados pessoais, sendo um importante avanço para o comércio exterior e, portanto, para o desenvolvimento econômico do Brasil.

A aplicação efetiva do direito individual fundamental à privacidade depende, em grande medida, das respostas coletivas que serão apresentadas para implementá-lo, motivo pelo qual é necessário empenhar-se na construção de uma democracia da informação que proteja tanto a autodeterminação e a liberdade de controle das informações pessoais pelo cidadão, como também a tutela contra a utilização discriminatória dos dados. Nesse contexto, a minuta ora apresentada visa possibilitar que a sociedade brasileira obtenha os benefícios econômicos e sociais potencializados pela tecnologia da informação, ao criar no país uma arquitetura

regulatória capaz de fazer emergir o tema da proteção de dados pessoais como um verdadeiro vetor de políticas públicas, composto por instrumentos estatutários, sancionatórios, bem como por um órgão administrativo, responsável pela implementação e aplicação da legislação.

A consolidação de um regime integrado de proteção de dados no Brasil mostra-se, assim, fundamental no ordenamento jurídico pátrio, de modo a possibilitar uma regulação integral do tema e a coesão de diversas iniciativas na área. Somente uma regulação geral assegurará a instituição de princípios harmônicos sobre o tema, proporcionando o controle dos riscos envolvidos no processamento de dados e assegurando o controle do cidadão em relação às suas próprias informações pessoais e, assim, garantindo a necessária segurança jurídica para a atividade empresarial e para a administração pública no tratamento de dados pessoais.

GABRIEL REIS CARVALHO

Diretor do Departamento de Proteção e Defesa do Consumidor, Substituto