Comentários ao Anteprojeto de Lei sobre Proteção de Dados Pessoais

Renato Leite Monteiro

Advogado do escritório Opice Blum Advogados Associados, atuante na área do Direito Eletrônico com ênfase no uso da Internet e de novas tecnologias. Membro da Comissão de Informática Jurídica da OAB/CE. Membro fundador do Instituto Brasileiro de Direito da Tecnologia da Informação. Mestre em Direito Constitucional pela Universidade Federal do Ceará. Professor da Escola Autônoma de Direito de São Paulo (FADISP). Palestrante convidado em eventos nacionais e internacionais.

Contato: opiceblum.rmonteiro@opiceblum.com.br
@RenatoLMonteiro

Caio César Carvalho Lima

Advogado do escritório Opice Blum Advogados Associados, atuante na área do Direito Eletrônico com ênfase no uso da Internet e de novas tecnologias. Membro da Comissão de Informática Jurídica da OAB/CE. Secretário-Geral do Instituto Brasileiro de Direito da Tecnologia da Informação. Especialização *lato sensu* em Direito da Tecnologia da Informação. Palestrante convidado em eventos nacionais e internacionais, com artigos e capítulos de livro publicados sobre o tema.

Contato: opiceblum.caio@opiceblum.com.br
@CaioCCLima

SUMÁRIO

INTRODUÇÃO..... 3

JUSTIFICATIVA..... 5

ASPECTOS PRINCIPAIS..... 5

TÍTULO I DA TUTELA DOS DADOS PESSOAIS 6

CAPÍTULO I DISPOSIÇÕES GERAIS 6

CAPÍTULO II PRINCÍPIOS GERAIS DE PROTEÇÃO DE DADOS.....11

CAPÍTULO III REQUISITOS PARA O TRATAMENTO DE DADOS PESSOAIS13

CAPÍTULO IV DOS DIREITOS DO TITULAR.....18

CAPÍTULO V TRATAMENTO DE DADOS SENSÍVEIS 22

CAPÍTULO VI SEGURANÇA DOS DADOS 24

CAPÍTULO VII COMUNICAÇÃO E INTERCONEXÃO DOS DADOS PESSOAIS 28

CAPÍTULO VIII DO TÉRMINO DO TRATAMENTO DOS DADOS PESSOAIS.30

CAPÍTULO IX TRATAMENTO DE DADOS PESSOAIS NO SETOR PÚBLICO .32

CAPÍTULO X TRATAMENTO DE DADOS PESSOAIS NO SETOR PRIVADO..34

CAPÍTULO XI TRANSFERÊNCIA INTERNACIONAL DE DADOS.....35

TITULO II TUTELA ADMINISTRATIVA 37

CAPÍTULO I AUTORIDADE DE GARANTIA 37

CAPÍTULO II SANÇÕES ADMINISTRATIVAS 40

TITULO III CÓDIGOS DE BOAS PRÁTICAS..... 42

TITULO IV DISPOSIÇÕES FINAIS E TRANSITÓRIAS..... 43

CONCLUSÃO..... 45

ENCERRAMENTO 47

INTRODUÇÃO

O Brasil, em contramão a muitos de seus pares no cenário mundial, ainda não dispõe de proteção adequada para dados de natureza pessoal. Mesmo levando em consideração as proteções à intimidade e à privacidade estabelecidas pela Constituição Federal e pelo Código Civil, e o amparo aos dados consumeristas, imposto pelo Código de Defesa do Consumidor, estamos muito distantes do nível de adequação garantido por legislações estrangeiras, como da Argentina, do México, dos EUA e da Europa.

Visando estabelecer um marco regulatório adequado, foi colocado em discussão o presente Anteprojeto de Lei de Proteção de Dados Pessoais, fruto de trabalho exemplar e louvável da Fundação Getúlio Vargas e do Ministério da Justiça. Teve por base diversas leis já em vigência no âmbito internacional, tais como a Diretiva Europeia de Proteção de Dados Pessoais (EC 95/46) e a Lei de Proteção de Dados Canadense.

Questiona-se se realmente é necessário tal marco legal. Essa dúvida pode ser respondida de forma mais eficaz por meio de um viés pragmático. O atual estágio tecnológico, o qual torna a utilização, por exemplo, da Internet algo quase que onipresente, a qual para seu funcionamento basal tem por costume a utilização massiva de dados de natureza pessoal (muitos deles sensíveis, como cor, sexo e orientações políticas), enseja a imperatividade de um correto tratamento desses dados.

Podemos vislumbrar quase que diariamente na mídia notícias de vazamento de dados pessoais, cadastrais e/ou financeiros. Analisando-se compilação de casos das chamadas *data breaches*[1], observa-se que já chega a quase 600 milhões o número de registros, levando-se em consideração apenas os países que compelem a publicização desses incidentes, o que não inclui o Brasil. O prejuízo oriundo dessa quantidade absurda de falhas de segurança é imensurável.

[1] http://www.privacyrights.org/data-breach#Total

Por um viés econômico, balizas legais garantem o princípio da segurança jurídica, o que por si tem consequências financeiras visíveis, uma vez que os investidores podem ter noção de como o mercado se comporta, em face das manobras comerciais desejadas por eles.

Inobstante, o maior beneficiário do estabelecimento de um marco legal é o cidadão, ente hipossuficiente nas relações travados com empresas e com o Estado. Este poderá ter as informações que compõem suas esferas de intimidade e privacidade tratadas adequadamente, garantindo que apenas o que é do seu interesse seja revelado ou utilizado por terceiros, garantindo a aplicação de direitos fundamentais e humanos.

A vigência de uma normativa que garanta esse nível de proteção não terá o condão de engessar ou de impedir o caráter autorregulatório da maioria das iniciativas tecnológicas. Pelo contrário, incentivará a criatividade e a novidade, assim como a neutralidade da rede, na medida em que estabelecerá regras claras para todos os jogadores do mercado.

O presente comentário traz em si pequenos trechos de discussões oriundas do recém formado grupo de estudos sobre privacidade e novas tecnologias.

JUSTIFICATIVA

O presente comentário se justifica em face da premente necessidade de promulgação de uma Lei de Proteção de Dados Pessoais que conte com contribuições ativas de diversos espectros da sociedade.

O Ministério da Justiça, por meio de fórum público de discussões, possibilitou a interessados exporem seus comentários e sugestões ao presente projeto de lei, por meio de um método dialético, visando uma melhor adequação aos reais anseios da sociedade.

O texto permaneceu aberto para que todos da população disponibilizassem seus comentários acerca das prescrições, a fim de que se conseguisse atingir a redação que melhor se adequasse aos anseios da sociedade.

ASPECTOS PRINCIPAIS

O presente comentário levou em consideração alguns aspectos principais, visto que a discussão de todos os pormenores da lei daria ensejo a uma compilação enciclopédica. Entre os pontos nervais estão: **(a)** a falta de estabelecimento de um tempo mínimo para a guarda de registros de natureza pessoal; **(b)** a discussão acerca da utilização de documentos eletrônicos e físicos; **(c)** a possibilidade de requisição de informações sem a presença de advogado; **(d)** o armazenamento de dados pessoais, para fins estatísticos e a utilização desses dados para fins comportamentais; e **(e)** a necessidade de uma transparência mais eficaz nos procedimentos, mormente dos métodos utilizados para a coleta da anuência do titular dos dados pessoais.

COMENTÁRIOS

DISPÕE SOBRE A PROTEÇÃO DE DADOS PESSOAIS, A PRIVACIDADE E DÁ OUTRAS PROVIDÊNCIAS

COMENTÁRIO: O título do presente projeto de lei deve abarcar também a proteção à intimidade, tendo por base a teoria alemã dos 03 círculos, que faz a separação entre segredo, intimidade e privacidade. Levando em consideração que o texto aqui discutido também discorre sobre dados sensíveis, que podem estar, inclusive, dentro da própria esfera de segredos, e levando em consideração que o tema-título do projeto de lei, como um *caput* de todo o texto, pode funcionar como norte interpretativo da norma, o termo intimidade deve ser incluído.

O CONGRESSO NACIONAL decreta:

TÍTULO I DA TUTELA DOS DADOS PESSOAIS

CAPÍTULO I DISPOSIÇÕES GERAIS

Art. 1. Esta lei tem por objetivo garantir e proteger, no âmbito do tratamento de dados pessoais, a dignidade e os direitos fundamentais da pessoa, particularmente em relação à sua liberdade, igualdade e privacidade pessoal e familiar, nos termos do art. 5º, incisos X e XII da Constituição Federal.

COMENTÁRIO: Nos mesmos moldes do exposto sobre o título do presente projeto de lei, entendemos ser necessária a inclusão nesse artigo do termo intimidade, em confluência com o art. 5º, inciso X da CF/88. Além do mais, o objetivo da presente lei não é somente a proteção dos dados pessoais, mas também o estabelecimento de um paradigma jurídico que possa servir de sustentáculo, também, para investimentos econômicos e desenvolvimento tecnológico, ao mesmo tempo em que protege o cidadão e o consumidor. Desta forma, o presente artigo também poderia contemplar a proteção econômica e consumerista.

Art. 2. Toda pessoa tem direito à proteção de seus dados pessoais.

COMENTÁRIO: A presente lei tem por objetivo a proteção de dados pessoais de pessoa física. Inobstante o Código Civil em seu art. 52 igualar a

proteção dos direitos de personalidade das pessoas físicas e jurídicas, as leis que discorrem sobre os diferentes tipos societários já trazem em seu bojo proteções especificas, além da lei de Propriedade Industrial (Lei 9.279/1996) e das normas de Direito Concorrencial.

O presente texto foi elaborado tendo por base leis que protegem a pessoa física, tais como a Diretiva Europeia EC 95/46 e a Lei de Proteção de Dados Canadense. Apenas para fins de teleologia da norma, entendemos ser necessário incluir o termo "pessoa física", com o objetivo de evitar que método interpretativo venha a expandir o espectro de atuação da norma.

Art. 3. A presente lei aplica-se aos tratamentos de dados pessoais realizados no território nacional por pessoa física ou jurídica de direito público ou privado, ainda que o banco de dados seja localizado no exterior.

§ 1º A presente lei não se aplica:

I – ao tratamento de dados pessoais realizado por pessoa física para fins exclusivamente pessoais e domésticos, desde que os dados tratados não sejam destinados à comunicação;

II – aos bancos de dados utilizados para o exercício da atividade jornalística e exclusivamente para tal fim.

§ 2º Os bancos de dados instituídos e mantidos para fins exclusivos de segurança pública, defesa, segurança do Estado e suas atividades de investigação e repressão de delitos serão regidos por legislação específica.

COMENTÁRIO: A abrangência do presente artigo, incluindo bancos de dados ou base de dados que se encontrem no exterior, condiz com a atual tendência tecnológica da ubiquidade, mormente com a utilização de *Cloud Computing*, em que os dados podem estar armazenados nos mais diversos locais. É prática do mercado o não fornecimento dessas informações, mesmo quando requisitadas judicialmente, se elas estiverem alocadas em território alienígena.

Ainda, importante incluir no texto do artigo o termo "base de dados", visto existirem diferenças entre "banco de dados" e "base de dados", como podemos vislumbrar na Lei de Direitos Autorais (Lei 9.610/1998), que

garante a proteção, em seu art. 7º, inc. XII, às bases de dados. Novamente, importante ter em mente a teleologia da norma.

Complementando o presente artigo está o art. 39, XII, do APL (anteprojeto de lei), que discorre sobre a competência da Autoridade de Garantia (AG) para atestar a equivalência entre os países com relação à proteção aos dados pessoais e permitir a transferência de dados entre estes países.

Art. 4. Para os fins da presente lei, entende-se como:

I - dado pessoal: qualquer informação relativa a uma pessoa identificada ou identificável, direta ou indiretamente, incluindo todo endereço ou número de identificação de um terminal utilizado para conexão a uma rede de computadores;

II - tratamento: toda operação ou conjunto de operações, realizadas com ou sem o auxílio de meios automatizados, que permita a coleta, armazenamento, ordenamento, conservação, modificação, comparação, avaliação, organização, seleção, extração, utilização, bloqueio e cancelamento de dados pessoais, bem como o seu fornecimento a terceiros por meio de transferência, comunicação ou interconexão;

III - banco de dados: todo conjunto estruturado de dados pessoais, localizado em um ou vários locais, em meio eletrônico ou não;

IV - dados sensíveis: dados pessoais cujo tratamento possa ensejar discriminação do titular, tais como aqueles que revelem a origem racial ou étnica, as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação sindical, partidária ou a organizações de caráter religioso, filosófico ou político, os referentes à saúde e à vida sexual, bem como os dados genéticos e biométricos;

V - titular: pessoa física a quem se referem os dados pessoais que são objeto de tratamento nos termos desta lei;

VI - responsável: a pessoa física ou jurídica, de direito público ou privado, a quem competem as decisões referentes às finalidades e modalidades de tratamento de dados pessoais;

VII - subcontratado: a pessoa jurídica contratada pelo responsável pelo banco de dados como encarregado do tratamento de dados pessoais;

VIII - comunicação: ato de revelar dados pessoais a um ou mais sujeitos determinados diversos do seu titular, sob qualquer forma;

IX - difusão: ato de revelar dados pessoais a um ou mais sujeitos indeterminados diversos do seu titular, sob qualquer forma;

X - interconexão: transferência de dados de um banco de dados a outro, mantido ou não pelo mesmo proprietário, com finalidade semelhante ou distinta;

XI - bloqueio: a conservação do dado pessoal ou do banco de dados com a suspensão temporária de qualquer operação de tratamento;

XII - cancelamento: a eliminação ou destruição de dados ou conjunto de dados armazenados em banco de dados, seja qual for o procedimento empregado;

XIII - dissociação: ato de modificar o dado pessoal de modo a que ele não possa ser associado, direta ou indiretamente, com um indivíduo identificado ou identificável;

XIV - dados anônimos: dados relativos a um titular que não possa ser identificado, nem pelo responsável pelo tratamento nem por qualquer outra pessoa, tendo em conta o conjunto de meios suscetíveis de serem razoavelmente utilizados pelo responsável pelo tratamento dos dados ou por qualquer outra pessoa para identificar o referido titular;

COMENTÁRIO: O presente artigo tem por objetivo conceituar os diversos termos utilizados ao longo do texto da norma. Entre as várias sugestões de adequação, seguem algumas:

- Alterar, no inc. I, o termo "terminais" para "dispositivos", visto que este tem uma maior abrangência e encontra-se em confluência com a chamada "internet das coisas";

- Alterar o inc. VII para que seja incluído o termo "pessoa física", visto que esta também pode ser subcontratada para realizar o tratamento de dados pessoais (ligação direta com o art. 25);

- Entendemos ser necessária a inclusão de alguns termos, como um que trate diretamente sobre a anuência do cidadão (*opt-in*), visto que ele é por diversas vezes citado ao longo do texto e é peça fundamental para que seja possível o adequado e devido tratamento dos dados pessoais.

- Outra grande discussão atual, que inclusive conta com grupos de trabalhos específicos na revisão da Diretiva Europeia, são dados

oriundos de registros de geolocalização, que podem, todavia, estar incluídos no conceito primeiro de dados pessoais, se deles for possível individualizar uma pessoa. Caso não seja possível a individualização, contudo, o mero conjunto de dados geográficos em conjunto com outros dados comportamentais pode atingir uma coletividade, e influenciar o seus hábitos, devendo, portanto, receber proteção específica.

- Ainda sobre o inciso I, questiona-se se na conceituação de dado pessoal deveriam ser incluídos os registros de IP, uma vez que ele identificam o dispositivo utilizado, e não o indivíduo em si. Todavia, advogamos pela manutenção do texto com essa abrangência, em dissonância com demais legislações estrangeiras, visto que a agregação de dados com o número IP pode levar à identificação de um indivíduo.

Art. 5. O tratamento de dados pessoais por parte de pessoas jurídicas de direito público é permitido para o cumprimento de suas funções institucionais, dentro dos limites da lei.

COMENTÁRIO: Este artigo faz a delimitação entre pessoas jurídicas de Direito Público e Direito Privado. Discutiu-se se deveriam ser incluídas nesse tópico as pessoas jurídicas de direito privado de caráter público, como as sociedades mistas. Entendemos tal ser desnecessário, pois para fins de Direito estas são pessoas jurídicas de Direito Privado e estão limitadas pelos comandos da presente norma. A prevalência do presente artigo vem apenas a corroborar o fato de que qualquer pessoa jurídica, pública ou privada, pode ser responsabilizada pelo tratamento de dados pessoais.

Art. 6. O tratamento de dados pessoais é atividade de risco e todo aquele que, por meio do tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, é obrigado a ressarci-lo, nos termos da lei.

COMENTÁRIO: O presente artigo coloca em xeque discordância jurisprudencial e doutrinária sobre se o simples fato de as empresas exercerem atividade de risco ensejaria responsabilidade objetiva. Em

muitos *decisuns* dos tribunais pátrios, a responsabilidade objetiva vem sendo mitigada, em contraponto ao art. 927, parágrafo único do Código Civil, em face da natureza específica exercida pela atividade, como no caso de controle prévio de conteúdo gerado por usuários em redes sociais.

Todavia, no caso de tratamento de dados pessoais, o texto da norma foi ao encontro do atual Código Civil, pois determina que a atividade aqui descrita é atividade de risco e, portanto, sob os auspícios da responsabilidade objetiva, na qual não se faz necessária a prova da existência de culpa, negligência ou imperícia, apenas o nexo causal e o dano.

Este artigo demonstra a necessidade da presente lei como forma de estabelecer os basilares jurídicos a serem aplicados nos casos práticos. Eventuais exceções a esta regra já se encontram dispostas em nosso ordenamento jurídico, mormente no CDC, que funciona como norma cogente de aplicação horizontal, ao estabelecer os casos de culpa exclusiva da vítima e de falta de nexo causal entre o fornecedor e o dano.

Art. 7. A defesa dos interesses e direitos dos titulares de dados poderá ser exercida em juízo individualmente ou a título coletivo, na forma do disposto nos artigos 81 e 82 da Lei 8.078, de 11 de setembro de 1990, na Lei 7.347 de 24 de julho de 1985 e nos demais instrumentos de tutela coletiva estabelecidos em Lei.

COMENTÁRIO: Este artigo vai ao encontro ao que estabelece o art. 1º do CDC, que determina ser o Código de Defesa do Consumidor norma de ordem pública e de interesse social, que permite a aplicação horizontal intranormas e a defesa de interesses coletivos.

CAPÍTULO II PRINCÍPIOS GERAIS DE PROTEÇÃO DE DADOS

Art. 8. Os responsáveis pelo tratamento de dados pessoais deverão atender, dentre outros, aos seguintes princípios gerais de proteção de dados pessoais:

I - Princípio da finalidade: a não utilização dos dados pessoais objeto de tratamento para finalidades distintas ou incompatíveis com aquelas que fundamentaram a sua coleta e que tenham sido informadas ao titular; bem como a limitação deste tratamento às finalidades determinadas, explícitas e legítimas do responsável;

II - Princípio da necessidade: a limitação da utilização de dados pessoais ao mínimo necessário, de forma a excluir o seu tratamento sempre que a finalidade que se procura atingir possa ser igualmente realizada com a utilização de dados anônimos ou com o recurso a meios que permitam a identificação do interessado somente em caso de necessidade;

III - Princípio do livre acesso: a possibilidade de consulta gratuita, pelo titular, de seus dados pessoais, bem como de suas modalidades de tratamento;

IV - Princípio da proporcionalidade: o tratamento de dados pessoais apenas nos casos em que houver relevância e pertinência em relação à finalidade para a qual foram coletados;

V - Princípio da qualidade dos dados: a exatidão dos dados pessoais objeto de tratamento, com atualização realizada segundo a periodicidade necessária para o cumprimento da finalidade de seu tratamento;

VI - Princípio da transparência: a informação ao titular sobre a realização do tratamento de seus dados pessoais, com indicação da sua finalidade, categorias de dados tratados, período de conservação destes e demais informações relevantes;

VII - Princípio da segurança física e lógica: o uso, pelo responsável pelo tratamento de dados, de medidas técnicas e administrativas proporcionais ao atual estado da tecnologia, à natureza dos dados e às características específicas do tratamento, constantemente atualizadas e aptas a proteger os dados pessoais sob sua responsabilidade da destruição, perda, alteração e difusão, acidentais ou ilícitas, ou do acesso não autorizado;

VIII - Princípio da boa-fé objetiva: o respeito à lealdade e à boa-fé objetiva no tratamento de dados pessoais; e

IX - Princípio da responsabilidade: a reparação, nos termos da lei, dos danos causados aos titulares dos dados pessoais, sejam estes patrimoniais ou morais, individuais ou coletivos.

X – Princípio da prevenção: o dever do responsável de, para além das disposições específicas desta Lei, adotar, sempre que possível, medidas capazes de prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

COMENTÁRIO: Sugerimos, coadunando com a sugestão dada pelo Dr. Roberto Senise Lisboa, que deveria ser incluído como principio o da interpretação mais favorável para quem autoriza o tratamento de seus dados pessoais. Outros seriam desnecessários, como o da boa-fé objetiva ou da responsabilidade, visto que a sua aplicação é implícita, decorrente da Constituição Federal e do Código Civil.

CAPÍTULO III REQUISITOS PARA O TRATAMENTO DE DADOS PESSOAIS

Art. 9. O tratamento de dados pessoais somente pode ocorrer após o consentimento livre, expresso e informado do titular, que poderá ser dado por escrito ou por outro meio que o certifique, após a notificação prévia ao titular das informações constantes no art. 11.

§ 1º Nos serviços de execução continuada, o consentimento deverá ser renovado periodicamente, nos termos do regulamento.

§ 2º O tratamento de dados pessoais de crianças somente será possível com o consentimento dos responsáveis legais e no seu melhor interesse, sendo vedada a utilização destes dados para finalidades comerciais.

COMENTÁRIO: O presente artigo fala de ponto nerval do projeto de lei, ao tratar sobre a necessidade de aceitação expressa do titular dos dados pessoais. O conceito de consentimento, para fins da presente lei, deve ser melhor trabalhado, visto que mesmo com o disposto no art. 12, que determina que o *opt-in* deve estar em apartado, diversas são as formas possíveis de anuência do titular, e muitas delas podem ser obscuras, mesmo estando de acordo com a lei.

A presente norma, *verbi gratia*, não discorre sobre a possibilidade de *opt-in* prévio por meio de mensagem não requisitada com o objetivo de conseguir a anuência para o tratamento dos dados. Alguns países da Europa já estabeleceram, inclusive, o *double opt-in,* como forma mais efetiva de proteção. Prática comum no mercado, por exemplo, são os *checkbox* de *opt-in* já selecionados, como forma diversa de adesão, sem possibilidade de modificação.

Estudos mostram que poucos são os usuários que têm conduta ativa diversa do fornecimento de dados, quando da contratação de um serviço, o que traz em si forma automática de consentimento, metodologia divergente do que pretende a presente lei.

Entendemos, ainda, que o consentimento para utilização dos dados com fins comerciais deve ser colocado em tópico específico, garantido a correta

utilização deles, no caso de contratos de adesão expostos em *disclaimers* em sítios virtuais.

Interessante diferenciar no presente artigo criança e adolescente, e incluir esta última, para fins de consonância com o Estatuto da Criança e do Adolescente. Isso vem ao encontro das mais recentes discussões que vêm sendo tratadas na Comunidade Europeia, acerca da reformulação da Diretiva 95/46, hodiernamente em discussão.

Art. 10. O consentimento pode ser revogado a qualquer momento.

COMENTÁRIO: Em consonância com o CDC, art. 43, quando trata sobre a obrigação de retirar dos bancos de dados informações pessoais, quando não for mais do interesse do consumidor.

Art. 11. No momento da coleta de dados pessoais, o titular será informado de forma clara e explícita sobre:

I - a finalidade para a qual os seus dados pessoais estão sendo coletados e de que forma serão tratados;

II – a identidade e o domicílio do responsável pelo tratamento;

III - a natureza obrigatória ou facultativa do fornecimento dos dados;

IV - as conseqüências de uma eventual negativa em fornecê-los;

V - os sujeitos para os quais os dados podem ser comunicados e o seu âmbito de difusão; e

VI - os seus direitos, em particular da possibilidade de negar-se a fornecer os dados pessoais e sobre o seu direito de acesso e retificação gratuitos.

Parágrafo único. Considera-se nulo o consentimento prestado caso as referidas informações tenham conteúdo enganoso ou não tenham sido fornecidas de forma clara e explícita.

COMENTÁRIO: Este artigo impõe os requisitos necessários para conseguir a anuência do titular dos dados pessoais para que o tratamento deles. Todavia, não impõe de forma clara e explícita como isso se daria, anulando a eficácia do seu parágrafo único e proporcionando a prática de condutas obscuras como atualmente verificado.

Sugerimos que da mesma forma que o CDC impôs a necessidade de fonte de tamanho no mínimo 12 em contratos de adesão (art. 54, § 3º), delimite-se uma forma mínima para que o titular seja adequadamente informado. Tal tarefa pode ser repassada à Autoridade de Garantia, na função regulamentadora dos requisitos mínimos de segurança.

Art. 12. O consentimento, caso prestado em conjunto com outras declarações, deve figurar de forma expressa e apartada.

COMENTÁRIO: Recai no mesmo encalço do art. 9º, não delimitando a forma de como deve ser conseguido o consentimento, mas aumenta a efetividade ao colocá-lo em lugar separado, diferente dos contratos de adesão. Para uma maior segurança, sugerimos que o mecanismo de o*pt-in* esteja também em apartado e não previamente selecionado, como vem se constatando recentemente.

Art. 13. O consentimento será dispensado quando o tratamento:

I - for necessário para a execução de obrigações derivadas de um contrato do qual é parte o titular, para a execução de procedimentos pré-contratuais requeridos por este, ou para o cumprimento de uma obrigação legal por parte do responsável;

II - referir-se a dados provenientes de registros, atos ou documentos públicos de acesso público irrestrito;

III - for necessário para o exercício de funções próprias dos poderes do Estado;

IV - for realizado unicamente com finalidades de pesquisa histórica, científica ou estatística;

V - for necessário para a proteção da vida ou da incolumidade física do titular ou de um terceiro, nos casos em que o titular não possa prestar o próprio consentimento por impossibilidade física ou por incapacidade de compreensão;

VI - for necessário para o exercício do direito de defesa ou para fazer valer um direito em sede judicial, desde que os dados coletados sejam tratados exclusivamente para esta finalidade e estritamente pelo período de tempo necessário para sua execução;

VII - disser respeito a dados sobre o inadimplemento de obrigações por

parte do titular, caso em que o titular deverá ser notificado previamente por escrito, nos termos do art. 43 da Lei 8.078/90 – Código de Defesa do Consumidor.

COMENTÁRIO: Elencando os casos em que o consentimento será dispensado, devemos ter por mente o inciso IV, que discorre sobre o tratamento de dados para fins estatísticos. Atualmente, o setor de análise comportamental tem por base justamente dados estatísticos coletados de indivíduos que tiveram suas informações dissociadas.

Chamada de *behavioral analysis*, essa metodologia utiliza, principalmente, dados coletados durante a navegação de usuários em sítios virtuais. São obtidas por meio de *cookies* ou mesmo de registros de pesquisas, que permitem traçar perfis de grupos específicos, e podem levar à individualização, com base em cruzamento de dados. A análise estatística de comportamento virtual pode influenciar toda uma coletividade e atingir diretamente os hábitos de indivíduos, principalmente os comerciais.

Dados como número de usuários, de determinada região, em certo horário, que utilizaram determinado serviço, são tão relevantes como dados não dissociados. Portanto, necessário fazer diferenciação de que tipo de análise estatística prescinde de anuência para ser tratada.

Crítica também deve ser feita ao inciso VII, pois novamente recorre a meios físicos e escritos, mesmo que esteja nos molde do art. 43 do CDC. Necessário rever essa metodologia ou determinar casos em que a comunicação pode se dar de forma totalmente eletrônica.

Art. 14. Os dados pessoais que forem objeto de tratamento deverão ser:
I - tratados de forma lícita e com boa-fé;

II - coletados e armazenados para finalidades determinadas, explícitas e legítimas;

III – exatos, claros, objetivos, atualizados e de fácil compreensão;

IV - pertinentes, completos, proporcionais e não excessivos em relação à finalidade que justificou sua coleta ou tratamento posterior;

V - conservados de forma a permitir a identificação de seu titular por um período de tempo não superior ao necessário para as finalidades que justificaram sua coleta ou tratamento posterior; e

VI - conservados por período não superior ao estabelecido em lei ou regulamento específico para cada setor.

§ 1º É vedado o tratamento de dados pessoais obtidos por meio de erro, dolo, coação e lesão.

§ 2º Os dados pessoais obtidos ou tratados de forma contrária à presente lei e à disciplina referente à proteção de dados não poderão ser utilizados e deverão ser cancelados.

COMENTÁRIO: O artigo 14 apenas repete os princípios norteadores do tratamento de dados pessoais, já expostos no art. 8º. Todavia, em seu inciso V, ao dispor sobre o tempo de armazenamento dos dados pessoais, recai sobre a mesma problemática enfrentada atualmente pelos tribunais, pela doutrina e pelo Marco Civil da Internet Brasileira. Ao determinar que os dados não podem ser conservados por período de tempo superior ao necessário para as finalidades que justificaram sua coleta, o texto repassa para a Autoridade de Garantia ou para as instituições cabíveis a determinação deste prazo.

O art. 14 do Marco Civil determina que os registros eletrônicos de conexão não podem ser armazenados por período superior a 6 (seis) meses. Sem adentrar na seara da discussão se tal período é ou não suficiente, a questão maior diz respeito à falta de obrigatoriedade imposta na conservação dos registros, após uma leitura literal do texto.

As empresas que detém dados de conexões de acesso à Internet, que nos moldes do art. 4º, I, do presente texto também tratam dados pessoais, não estariam, assim, compelidas a efetuar qualquer tipo de armazenamento desses dados, o que impossibilitaria qualquer elucidação de ilícitos levados a efeito com o uso de meios eletrônicos, até mesmo para fins de responsabilidade civil.

Desta forma, advogamos pela menção expressa nas leis, de Dados Pessoais e no Marco Civil da internet, por um prazo mínimo de armazenamento,

repassando a obrigação para impor um prazo máximo às instituições responsáveis pelos diversos tipos de dados pessoais tratados.

Com relação à redação da norma, desnecessário o §1º, visto que tal obrigação já se encontra exposta no art. 9º, ao tratar sobre o consentimento do titular.

CAPÍTULO IV DOS DIREITOS DO TITULAR

Art. 15. O titular dos dados poderá obter do responsável pelo tratamento a confirmação da existência de dados pessoais que lhe digam respeito, bem como o acesso aos dados em si, tanto diretamente, como por meio da ação de *habeas data*, nos termos da lei.

§ 1º As informações requeridas serão fornecidas, imediatamente, de forma simplificada ou, no prazo de 5 (cinco) dias, por meio de um extrato claro e completo, abrangendo a informação sobre a sua origem, bem como sobre a lógica, os critérios utilizados e a finalidade do respectivo tratamento.

§ 2º O fornecimento destas informações não importa em ônus para o titular dos dados.

§ 3º Estas informações, por escolha do titular, poderão ser fornecidas por escrito ou por meio eletrônico, seguro e idôneo para tal fim.

§ 4º A informação deve ser ampla e versar sobre a totalidade do registro existente, mesmo quando o requerimento compreender somente um aspecto dos dados pessoais do titular.

§ 5º Os dados pessoais serão armazenados de forma que permitam o exercício do direito de acesso.

COMENTÁRIO: O art. 15 encontra-se nos moldes do art. 43 do CDC, inclusive com relação ao prazo de 05 (cinco) dias imposto para informar ao titular dos dados pessoais se qualquer informação ao seu respeito se encontra na base de dados do responsável pelo tratamento destes.

A parte final do *caput* do presente artigo determina que o acesso ao banco de dados poderá ser feito por meio do remédio constitucional do *Habeas Data*, que é peça processual adequada para ter acesso a banco de dados publico[2]. O art. 43, §4º do CDC, considera os bancos de dados de

[2] Lei n. 9507/97, Art. 1º (VETADO)

consumidores algo de caráter público. Em uma interpretação integrativa da lei, a presente norma, ao possibilitar o acesso aos bancos de dados de registros pessoais, por meio de *Habeas Data* confere caráter público a eles, mesmo que não tenham natureza consumerista. Nesse cenário, podemos imaginar situações como a da impetração desse remédio em face de uma pequena ONG, pelo simples fato desta lidar com dados de natureza pessoal. Advogamos por uma explicitação maior desse artigo.

O art. 15 dispõe, ainda, que é direito do titular o conhecimento da lógica aplicada para o tratamento de seus dados. Ou seja, o método aplicado. Todavia, o método, em muitos países, mormente nos EUA, recebe proteção autoral e industrial, não podendo, portanto, ser revelado a terceiro ou utilizado por este. Mesmo que esta proteção inexista, atualmente, no Brasil, poderíamos vir a ter um conflito entre normas de natureza nacional e internacional, o que pode levar a um impacto econômico. Se o Google revelar, por exemplo, por completo o seu algoritmo de procura, isso pode levá-lo a sucumbir perante seus concorrentes, tendo em vista a ampla divulgação de sua maior ferramenta computacional.

Para fins de requisição das informações e alteração destas, importante notar que em nenhum momento se limita a atuação em tais procedimentos por meio de um advogado constituído, o que nos leva a inferir que o cidadão, *sponte propria*, poderá propor tais procedimentos.

Art. 16. Mediante solicitação do titular dos dados, o responsável deverá, sem ônus, no prazo de 5 (cinco) dias:

I - corrigir os dados pessoais que forem incompletos, inexatos ou desatualizados;

II - cancelar, dissociar ou bloquear os dados pessoais que forem desnecessários, excessivos ou tratados em desconformidade com a presente lei.

Parágrafo único. O responsável obriga-se, no prazo de 5 (cinco) dias, a comunicar aos destinatários das informações a realização de correção,

Parágrafo único. Considera-se de caráter público todo registro ou banco de dados contendo informações que sejam ou que possam ser transmitidas a terceiros ou que não sejam de uso privativo do órgão ou entidade produtora ou depositária das informações.

cancelamento, dissociação e bloqueio dos dados.

COMENTÁRIO: Enquanto o artigo 15 discorre sobre a requisição de dados pessoais contidos em determinada base de dados, o art. 16 fala sobre a alteração dos dados já existentes. A crítica recai sobre a necessidade de fundamentação, quando do pedido de cancelamento, dissociação ou bloqueio, demonstrando que os dados ora fornecidos não são mais necessários para os fins originais. A necessidade de justificativa encontra-se em conflito com o art. 10, que determina que a revogação da anuência pode ser feita a qualquer momento, e não impõe mais nenhum requisito. Ao parágrafo único, para fins de simetria com o art. 15, §3º deve ser incluída a possiblidade de comunicação ao titular das alterações por via eletrônica ou escrita.

Art. 17. O titular dos dados poderá opor-se, total ou parcialmente, ao tratamento de seus dados pessoais:

I - sempre que tiver motivos legítimos, salvo nos casos em que o tratamento seja necessário para o cumprimento de uma obrigação imposta pela lei à pessoa responsável;

II - quando seus dados forem utilizados para fins publicitários, ainda que tenham sido submetidos a um procedimento de dissociação.

COMENTÁRIO: O presente artigo é louvável, uma vez que dá ao titular dos dados a possibilidade de completo controle sobre fornecer ou não suas informações. Todavia, merece algumas críticas. Primeiro, deve ser adicionada a obrigatoriedade de informar ao titular as consequências na prestação do serviço, caso persista na oposição ao tratamento, nos moldes do art. 11, IV. Esta pode ser uma forma de mitigar eventuais casos em que o titular irá se opor.

A necessidade de uma ferramenta que reduza esta oposição é necessária, uma vez que a impossibilidade de tratar os dados pode afetar diretamente a indústria, limitando a sua atuação, principalmente a de caráter publicitário. Tal discussão já esteve em foco quando da elaboração do Código de

Autorregulamentação para a Prática de *E-mail Marketing* (CAPEM)[3], que teve por escopo encontrar um método que pudesse ser menos invasivo e ao mesmo tempo ir ao encontro dos interesses comerciais das empresas. Desta forma, a inclusão de parágrafo impondo a obrigação de informar os eventuais reveses poderia vir a suprir essa limitação.

Art. 18. Nos casos de descumprimento desta lei, o titular poderá pleitear os seus direitos perante a Autoridade de Garantia, na forma do regulamento.

COMENTÁRIO: O artigo 18 cria uma nova instância administrativa, o que é benéfico ao titular dos dados pessoas, visto que essa entidade irá funcionar como ente regulador e fiscalizador do tratamento de dados pessoais. Temos assim, a possibilidade de vários procedimentos distintos, porém complementares, para perquirir o mesmo objetivo, qual seja, o acesso aos dados pessoais. Pode-se recorrer à **(a)** notificação à responsável pelo tratamento; **(b)** proposição de medida civil judicial; **(c)** proposição de requisição administrativa à Autoridade de Garantia; e **(d)** interposição de *Habeas Data*.

Art. 19. O titular dos dados tem direito a não ser submetido a decisões que lhe afetem, de maneira significativa, unicamente com base em um tratamento automatizado de dados pessoais destinado a definir o perfil ou a personalidade do titular.

§ 1º Qualquer decisão desta natureza pode ser impugnada pelo titular, que tem o direito de obter informações do responsável pelo tratamento a respeito dos critérios desta avaliação e sobre o procedimento em que esta se baseou.

§ 2º Admite-se esta modalidade de decisão nos casos em que tenha sido expressamente solicitada pelo titular e desde que garantidos o devido processo legal e a ampla defesa.

COMENTÁRIO: Reportamos aos comentários do art. 15, do art. 9º e do art. 17. O art. 19 pode ser inócuo, uma vez que a quase totalidade dos tratamentos atuais é feita de forma automatizada, sendo, posteriormente, os dados obtidos cruzados com outras informações, com o escopo de diferenciar indivíduos ou grupos de indivíduos.

[3] Informações completas podem ser obtidas em: <http://www.capem.org.br>.

CAPÍTULO V TRATAMENTO DE DADOS SENSÍVEIS

Art. 20. Nenhuma pessoa pode ser obrigada a fornecer dados sensíveis.

COMENTÁRIO: Dados sensíveis, para os fins da presente lei, são conceituados no art. 4º, IV. A crítica ao conceito aqui empregado recai sobre a ausência de dados geográficos, algo que será incluído na revisão da Diretiva Europeia. O elogia recai sobre a inclusão como dados sensíveis dos dados de natureza genética, algo que não foi vislumbrado em 1995, quando da edição da EC 95/46.

Art. 21. É proibida a formação de bancos de dados que contenham informações que, direta ou indiretamente, revelem dados sensíveis, salvo disposição legal expressa, respeitados os direitos de personalidade do titular, em especial a garantia de não discriminação.

§ 1º O tratamento de dados sensíveis será permitido quando:

I - o titular tiver dado o seu consentimento livre, informado e por escrito, sempre que este tratamento for indispensável para o legítimo exercício das atribuições legais ou estatutárias de seus responsáveis.

II - for realizado por associações e outras entidades sem fins lucrativos de natureza política, filosófica, religiosa ou sindical para a realização de finalidades lícitas e compreendendo os dados pessoais de seus inscritos, sempre que os dados não sejam comunicados ou difundidos para terceiros e quando o ente em questão determine medidas idôneas de garantia dos direitos do titular para o tratamento realizado;

III - for necessário para a proteção da vida ou da incolumidade física do titular ou de um terceiro, nos casos em que o titular não possa prestar o próprio consentimento por impossibilidade física ou por incapacidade de compreensão; ou

IV - for realizado unicamente com finalidades de pesquisa histórica, científica ou estatística;

V - for relativo a dados manifestamente tornados públicos pelo seu titular.

VI - for realizado por profissionais da área da saúde ou entidades sanitárias e se mostrar indispensável para a tutela da saúde do interessado.

VII – for necessário para o exercício de funções próprias dos poderes de Estado, previstas em lei.

§ 2º Em qualquer hipótese, considerar-se-á ilegal o tratamento de dados sensíveis que for utilizado para fins discriminatórios.

COMENTÁRIO: O art. 21 impõe proibição na formação de bancos de dados que contenham informações que possam levar a inferir dados sensíveis, salvo por expressa disposição legal. Desse trecho do artigo podemos afirmar que somente se lei diversa da presente permitir a criação desse tipo de base legal esta será permitida. Todavia, o §1º, inc. I do mesmo artigo afirma que o tratamento de dados sensíveis será permitido quando o titular tiver dado o seu consentimento livre quando este for necessário para a realização de suas atribuições legais ou estatutárias. Encontramos nesse trecho a possibilidade de ato particular suplantar comando legal, no caso das atribuições legais ou estatutárias não discorrerem expressamente sobre a possiblidade de fornecimento de dados sensíveis. É necessário, portanto, uma sincronia de textos legais para que seja viável o tratamento de dados sensíveis.

O inciso IV recebe as mesmas críticas, só que desta vez mais periclitantes, do que as opostas ao art. 13, IV, sobre os dados para fins meramente estatísticos.

O inciso VI precisa receber regulamentação específica dos órgãos condizentes, sejam eles de natureza sanitária ou de saúde. Inclusive, cumpre observar que o Conselho Federal de Medicina (CFM) já emitiu a Resolução Nº 1.821/07, aprovando as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde.

Art. 22. A Autoridade de Garantia poderá indicar medidas de segurança e de proteção ao titular de dados sensíveis que deverão ser adotadas pelo responsável pelo tratamento.

COMENTÁRIO: Necessidade de adequação tecnológica das empresas e dos regulamentos de segurança da informação e de privacidade dos responsáveis por tratamento de dados sensíveis. Necessário que os

responsáveis tenham em mente que essas medidas de segurança podem ser alteradas com o tempo, o que poderia ensejar a necessidade de planejamento financeiro vislumbrando modificações futuras.

CAPÍTULO VI SEGURANÇA DOS DADOS

Art. 23. O tratamento de dados pessoais será feito de modo a reduzir ao mínimo, mediante a adoção de medidas idôneas de segurança preventiva, o risco de sua destruição ou perda, de acesso não autorizado ou de tratamento não permitido pelo titular ou diverso da finalidade da sua coleta, independentemente do motivo.

Parágrafo único. As medidas referidas no caput devem ser proporcionais ao atual estado da tecnologia, à natureza dos dados e às características específicas do tratamento, em particular no caso do tratamento de dados sensíveis.

COMENTÁRIO: Importante observar a preocupação que aqui se teve com a questão da segurança da informação, tendo-se, inclusive, criado princípio próprio, o "Princípio da Segurança Física e Lógica" (art. 8º, VII), tema que, com a elevação do uso dos sistemas de tecnologia, vem adquirindo cada vez mais importância. Cumpre ter em mente o que diz respeito aos bancos de dados, principais repositórios de informações, que precisam ser desenhados de modo a impedir que, mesmo quando capturados por terceiros não autorizados, ainda assim, seja bastante difícil o acesso aos dados lá contidos, privilegiando-se a utilização de criptografia.

Cumpre observar, contudo, que se deve permitir o acesso a essas informações armazenadas, nos casos expressamente permitidos no anteprojeto, como consta no Capítulo V, antes referido, que aborda o "tratamento de dados sensíveis".

Por derradeiro, a previsão do parágrafo único, deve ser analisada de modo a se evitar a perpetuação de desníveis em termos de exigência. Isto é, caso se esteja diante de grandes bancos, que lidam com informações frequentemente alvos de criminosos, certamente, devem ter atenção mais elevado do que uma pequena loja que possui cadastros de seus clientes.

Atente-se, contudo, para o fato de que as previsões aqui trazidas não são hábeis a superar a necessidade de edição de lei específica tratando de crimes levados a efeito em ambiente Web, mesmo se levando em conta que, atualmente, cerca de 95% das condutas ilícitas práticas em meio eletrônico já são punidas com o ordenamento em vigor.

Todavia, adentrando na seara penal, e tendo por norte a aplicação mínima do direito penal, a simples criminalização de novas condutas pode não ser tão eficiente quanto a aplicação de medidas cíveis inibitórias.

Art. 24. Um conjunto de medidas mínimas de segurança preventiva será publicado pela Autoridade de Garantia dentro de, no máximo, um ano após a entrada em vigor da presente lei, e atualizado periodicamente, com base na evolução da tecnologia e na experiência adquirida.

COMENTÁRIO: Passando-se ao artigo 24, observa-se que ele traz medida salutar, ao passo em que reafirma a necessidade de constantes adaptações às alterações tecnológicas daqueles que lidam com dados pessoais. Ocorre que a espera de até 01 (um) ano para a publicação por parte da AG das medidas mínimas de segurança preventiva pode representar longo espaço de tempo em que a lei, praticamente, não terá suas prescrições efetivamente cumpridas.

Ademais, deve-se ter em mente que isso implicará, também, à AG que fique atenta às novidades trazidas em sede de normas da ABNT (Associação Brasileira de Normas Técnicas), ISO (Organização Internacional para Padronização), com especial atenção para as já publicadas normas ISO 27.001 e 27.002, previsões da *RSA Data Security*, RFC (*Request for Comments*), dentre outros. Nessa esteira, as Políticas de Segurança da Informação, bem como os Regulamentos Internos de Segurança da Informação – RISI e o Termos de Uso de Segurança da Informação - TUSI, presentes em inúmeras corporações, de igual modo, também precisarão ser sistematicamente atualizados, a fim de que sejam seguidas as prescrições legais mais recentes.

Ainda, pelo princípio da prevenção exposto no art. 8º, X, não limita os responsáveis a aguardar a publicação de recomendações de por parte da AG. Toda vez que for razoável segundo os costumes de mercado, devem estas se atualizar e garantir graus máximos de segurança aos dados tratados.

Art. 25. O **subcontratado** deve ter experiência, capacidade e idoneidade para garantir o respeito às disposições vigentes em matéria de tratamento de dados pessoais, e responderá solidariamente com o responsável pelos prejuízos causados pela sua atividade aos titulares dos dados.

Parágrafo único. O subcontratado deverá realizar o tratamento segundo as instruções fornecidas **por escrito** pelo responsável, que, mediante inspeções periódicas, verificará a observância das próprias instruções e das normas sobre a matéria.

COMENTÁRIO: A fim de melhor situar-se a *ratio legis* disposta no art. 25 do Anteprojeto, fundamental observarem-se as prescrições trazidas pelo art. 4º, VII, em que há a definição de subcontratado, bem como o art. 29, adiante melhor analisado, que aborda a responsabilidade solidária entre cedente e cessionário.

Diante disso, apenas com o intuito de trazer melhor clareza à redação do dispositivo, sugere-se a modificação do termo "subcontratado" para "administrador do banco de dados".

Outrossim, no parágrafo único, tem-se que o subcontratado deverá realizar o tratamento consoante as instruções fornecidas "por escrito". Tal anacronismo é recorrente ao longo do texto da norma, que trata os documentos eletrônicos de forma distinta dos textos escritos, como fica evidente no art. 15, §3º anteriormente já aludido.

Sobre o tema, sem prejuízo de diversos outros dispositivos que se posicionam favoravelmente à plena validade dessa documentação gestada em ambiente eletrônico (art. 225 do Código Civil, Medida Provisória 2.200-2/2001, Lei 11.419/2006), o Anteprojeto do Novo Código de Processo Civil,

Projeto 166/2010, também em debate na Internet[4], destacou a Seção VIII do Capítulo XI para abordar a questão, do que se observa não cumpre ser levada a efeito a distinção referida.

Art. 26 O responsável, o **subcontratado** ou qualquer outra pessoa que intervenha em qualquer fase do tratamento de dados pessoais obriga-se ao dever de segredo em relação aos mesmos, dever este que permanece após o término do respectivo tratamento ou do vínculo empregatício existente.

COMENTÁRIO: No art. 26 trouxe-se importante ressalva, acerca do necessário dever de segredo, *ad eternum*, em relação aos dados tratados, por parte daqueles que tiveram contato com eles. Mantém-se a ressalva anterior acerca da utilização do termo "subcontratado".

Essa característica é de grande relevância, principalmente se considerando que, em inúmeras oportunidades, pode-se ter contato com informações sensíveis que, caso liberadas sem qualquer preocupação, podem trazer inúmeros prejuízos às partes referidas.

Tal determinação coaduna com outros dispositivos legais do ordenamento pátrio, tais como o sigilo profissional, que encontra-se enquadrado em tipo penal exposto no art. 154 do Código Penal. Tal ressalva somente pode ser mitigada com autorização expressa do titular dos dados.

Art. 27. O responsável pelo tratamento deverá comunicar à Autoridade de Garantia e aos titulares dos dados, **imediatamente**, sobre o acesso indevido, perda ou difusão acidental, seja total ou parcial, de dados pessoais, sempre que este acesso, perda ou difusão acarretem riscos à privacidade dos seus titulares.

Parágrafo único. Nos casos mencionados no *caput*, a Autoridade de Garantia poderá tomar as providências que julgar necessárias, no âmbito de suas competências, inclusive determinando ao responsável a ampla divulgação do fato em meios de comunicação.

COMENTÁRIO: A leitura atenta do art. 27 traz a confirmação de que o tratamento de dados pessoais deve, efetivamente, passar a ser tema de

[4] Mais informações podem ser obtidas em: <http://participacao.mj.gov.br/cpc/>. Acesso em: 30 abr. 2011.

atenção recorrente das corporações, abordando-se a necessidade de imediata comunicação à AG e aos titulares dos dados, no caso de qualquer perda ou difusão deles, quer tenha sido total ou parcial.

Entende-se, contudo, que o termo "imediatamente" não se apresenta como o mais adequado, na medida em que não traça de forma concreta o lapso de tempo em que a parte deve acionar as partes referidas, fazendo-se necessário trazer prazo fixo, como 48 (quarenta e oito) horas, sendo tal prazo suficiente para serem tomadas as decisões que se fizerem necessárias.

Um dos maiores ativos de uma empresa é justamente a sua imagem perante o mercado. Este ativo determina, em muitos casos, a credibilidade que se detém. Por tal motivo, incidentes de segurança somente são divulgados amplamente e aos titulares quando houver obrigatoriedade legal para tanto, algo que somente pode ser levado a cabo se houve uma penalidade pela não persecução do ato. A determinação em divulgar e informar é premente nos ordenamentos de proteção de dados pessoais.

Todavia, quanto ao parágrafo único, entende-se que, em certos casos, a ampla divulgação do fato em meios de comunicação pode trazer inúmeros efeitos negativos, que suplantam os benefícios dessa atitude, por isso os casos devem ser analisados individualmente pela AG. Ademais, em todos os procedimentos levados a efeito no âmbito da Autoridade de Garantia, devem ser observados os princípios do Contraditório e da Ampla Defesa, insculpidos no art. 5º, LV, da Constituição Federal.

CAPÍTULO VII COMUNICAÇÃO E INTERCONEXÃO DOS DADOS PESSOAIS

COMENTÁRIO: Para que se consiga entender melhor o disposto no capítulo VII, importante observar as disposições dos arts. 43 a 44, que compõem a Seção VI do Código de Defesa do Consumidor, Lei 8.078/1990, que trata dos bancos de dados e cadastros de consumidores. Ademais, os conceitos de comunicação e de interconexão estão dispostos, respectivamente, nos incisos VIII e X do art. 4º do Anteprojeto.

Art. 28. A comunicação ou a interconexão dos dados pessoais somente será permitida com o consentimento livre e expresso do titular e para o cumprimento de fins diretamente relacionados com as funções legítimas do cedente e do cessionário.

§1º O consentimento para a comunicação ou interconexão é revogável a qualquer tempo.

§2º O consentimento será dispensado quando:

I - os dados forem provenientes de registros, atos ou documentos públicos acessíveis a qualquer pessoa, levando em consideração os limites estabelecidos para o acesso e publicidade destes dados;

II - para o cumprimento de uma obrigação prevista em lei;

III - quando for necessária para a proteção da vida ou da incolumidade física do titular ou de um terceiro, nos casos em que o titular não possa prestar o próprio consentimento por impossibilidade física ou por incapacidade de compreensão.

COMENTÁRIO: No *caput* do artigo 28 do projeto em análise, tem-se a regra geral sobre a comunicação e a interconexão dos dados pessoais, que somente serão permitidas com o consentimento livre e expresso do titular, para os fins relacionados com as funções legítimas do cedente e do cessionário.

Entende-se que se está seguindo as previsões constantes do Código de Defesa do Consumidor, especificamente do §3º do art. 43, que se manifesta no sentido de que "a abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele".

Em consonância com o presente artigo, e com o art. 43 do CDC, está a portaria número 05 de 2002 do Ministério da Justiça, que alargou o rol de cláusulas abusivas do art. 51 do CDC para contemplar:

> Art. 1º Considerar abusiva, nos contratos de fornecimento de produtos e serviços, a cláusula que:
>
> I - autorize o envio do nome do consumidor, e/ou seus garantes, a bancos de dados e cadastros de consumidores, sem comprovada notificação prévia;

II - imponha ao consumidor, nos contratos de adesão, a obrigação de manifestar-se contra a transferência, onerosa ou não, para terceiros, dos dados cadastrais confiados ao fornecedor;

III - autorize o fornecedor a investigar a vida privada do consumidor;

A permissão acima aludida é revogável a qualquer tempo, conforme dispõe o §1º do mesmo artigo. Cumpre estar atento, entretanto, para o que traz o art. 13 do anteprojeto, acima mencionado, em que se observam os casos de dispensa de consentimento para tratamento dos dados.

No que pertine à dispensa do consentimento, previsto no §2º do dispositivo, importante observar que, no inciso II, pode-se adicionar a previsão de dispensa de autorização, quando se estiver diante de obrigação contratual, e não apenas legal, como consta do texto hodierno, principalmente se levando em conta o *pacta sunt servanda*, não havendo violação do que traz o art. 104 do Código Civil, indo ao encontro, também, do que dispõe o art. 13, I. Por fim, o inciso III traz previsão sobre casos em que o titular não possa prestar o próprio consentimento, o que se faz necessária prévia comprovação desse estado, cumprindo ser analisado os arts. 4º e 5º do Código Civil, que tratam da personalidade e da capacidade.

Art. 29. O cessionário ficará sujeito às mesmas obrigações legais e regulamentares do cedente, inclusive quanto à responsabilidade solidária pelos danos eventualmente causados e ao dever de receber e processar impugnação e realizar correções.

COMENTÁRIO: O artigo aborda a questão da responsabilidade solidária, que não se presume, entre cedente e cessionário de dados pessoais, tema que se encontra disposto no Código de Defesa do Consumidor, no art. 25.

CAPÍTULO VIII DO TÉRMINO DO TRATAMENTO DOS DADOS PESSOAIS

Art. 30. Os dados pessoais serão cancelados quando deixarem de ser necessários ou pertinentes para a finalidade que justificou sua coleta e tratamento.

Parágrafo único. Lei ou regulamento poderá dispor sobre períodos máximos para o tratamento de dados pessoais em setores e situações específicas.

COMENTÁRIO: O artigo apresenta-se tecnicamente confuso, uma vez que, de sua leitura textual, tem-se a impressão de que, após certo tempo, os próprios dados pessoais seriam cancelados. Na verdade, o que se tem, é o cancelamento do tratamento deles. Diante disso, restou evidenciada lacuna no que toca à exclusão dos dados pessoais, a partir do momento em que eles não fossem mais necessários ou a guarda deles não fosse pertinente para as finalidades que justificaram a coleta deles.

No parágrafo único trouxe-se previsão de que lei ou regulamento trataria do prazo máximo para o tratamento de dados pessoais. Igualmente, o art. 14, V, em que se traz a previsão de que os dados pessoais deverão ser conservados de forma a permitir a identificação de seu titular por período de tempo não superior ao necessário, também não especificando qual seria esse lapso temporal.

Entende-se que, salvo melhor juízo, pelo menos alguma previsão específica sobre o tema deveria ser traçada, não sendo demais supor que o prazo máximo de 180 (cento e oitenta) dias seja razoável, fazendo-se analogia ao trazido no art. 14 do Marco Civil, quando tratou do dever do administrador do sistema de manter os registros de conexão pelo lapso referido. Ademais, nada obsta a que acordo entre as partes preveja prazo maior do que o sugerido, nunca podendo ser menor do que o aludido.

Importante, ainda, enaltecer que o presente texto legal também poderia discorrer sobre um prazo mínimo como forma de obrigação de armazenamentos de determinados registros após a anuência expressa de seus titulares.

Art. 31. No término do tratamento dos dados pessoais, sem prejuízo dos direitos do titular, e sempre que houver necessidade ou pertinência, os dados podem ser:

I - cedidos a terceiros, desde que destinados a tratamento para finalidades análogas àquelas para as quais foram colhidas e mediante o consentimento

dos titulares;

II - conservados para fins exclusivamente pessoais e não destinados à comunicação ou à difusão;

III - conservados ou cedidos a terceiro, unicamente para finalidades históricas, estatísticas ou de pesquisa científica.

COMENTÁRIO: O art. 31 trata de questões bastante delicadas, abordando no inciso I a cessão a terceiros dos dados, desde que haja consentimento dos titulares para tanto. Advoga-se que, no próprio instrumento em que houve a primeira autorização para tratamento das informações, já poderia constar a autorização para tal cessão, devendo-se, contudo, serem mantidas as finalidades para as quais foram colhidos precipuamente.

No inciso II, a referência aos fins exclusivamente pessoais é sobremaneira subjetiva, contradizendo-se com o art. 14, II, cumprindo ser melhor definido o que abrange essa disposição, sob pena de se dar ampla liberdade de se manejar essas informações. Em sendo assim, por ora, entende-se ser de bom alvitre remover o inciso.

Por fim, no que toca o ao inciso III, a previsão de conservação ou cessão deles para terceiros, quando diante de finalidades históricas, estatísticas ou de pesquisa científica, remetendo-se para aprofundamento o que já se observou no art. 13, IV. Da leitura do inciso, constata-se que não se fez qualquer menção à necessidade de consentimento do titular nesses casos, no que contradiz o que se trouxe no inciso I.

CAPÍTULO IX TRATAMENTO DE DADOS PESSOAIS NO SETOR PÚBLICO

Art. 32. A comunicação e interconexão de dados pessoais entre pessoas jurídicas de direito público será admitida nos casos em que suas competências não versem sobre matérias distintas, respeitados os direitos estabelecidos nesta lei.

Parágrafo único. A comunicação de dados pessoais entre pessoas jurídicas de direito público com competências sobre matérias distintas será admitida:

I - mediante expressa previsão legal, sempre no respeito aos direitos dos titulares dos dados; ou

II - quando for necessária para a realização das suas competências institucionais.

COMENTÁRIO: Passando-se ao art. 32, constata-se que ele trata da comunicação e da interconexão de dados pessoais entre pessoas jurídicas de direito público. Importante observar, de antemão, que a Constituição Federal protege e garante os direitos de privacidade e de intimidade, em seu art. 5º, X, devendo-se atentar para tal fato.

Ademais, o conceito de "matérias distintas" e de "competências institucionais" são sobremaneira abertos, abrindo margem para ampla liberdade de atuação, o que pode ter efeitos negativos até mesmo de graves consequências.

Ademais, não se exige qualquer autorização do titular dos dados para tal cessão, o que confirma a sensação de liberdade para troca dessas informações entre os distintos órgãos governamentais, ampliando as chances de vazamento desses dados.

Art. 33. Os responsáveis pelos bancos de dados públicos poderão, mediante decisão fundamentada e somente pelo período necessário, negar o cancelamento e a oposição ao tratamento dos dados pessoais, quando for indispensável para:

I - a proteção da ordem pública;

II – a proteção de direitos de terceiros;

III – não obstaculizar a atuação judicial ou administrativa em curso, vinculadas à investigação sobre o cumprimento de obrigações tributárias, o desenvolvimento de funções de controle da saúde e do meio ambiente e a verificação de infrações administrativas.

COMENTÁRIO: A norma trouxe conceito de banco de dados no art. 4º, III, sendo de leitura fundamental para amplo entendimento da temática. O dispositivo coaduna-se com o princípio da proporcionalidade, insculpido no art. 8, III, o qual, em linhas gerais, aborda o fato de que o direito de terceiros deve prevalecer sobre questões individuais.

Quanto ao inciso III, observe-se que ele reduz os casos em que os responsáveis pelos bancos de dados públicos poderão atuar, limitando-se ao cumprimento de questões tributárias, de saúde e meio ambiente ou infrações administrativas. Sugere-se que essas especificações sejam reduzidas, por tal representar restrições desnecessárias.

CAPÍTULO X TRATAMENTO DE DADOS PESSOAIS NO SETOR PRIVADO

At. 34. Toda entidade privada que realize o tratamento de dados pessoais para o desenvolvimento de suas atividades e conte com mais de duzentos empregados deverá apontar um diretor responsável pelo tratamento de dados pessoais.

§1º O diretor responsável pelo tratamento de dados pessoais deverá zelar, de forma independente, pela observância das disposições da presente lei.

§2º As atividades do diretor responsável pelo tratamento de dados pessoais consistem, entre outras, em:

I – atuar como o correspondente imediato da Autoridade de Garantia;

II - orientar os demais funcionários a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

III - manter uma relação dos tratamentos de dados pessoais realizados pela empresa, imediatamente acessível pelos titulares que requisitem seus próprios dados pessoais.

§3º A entidade informará à Autoridade de Garantia sobre a identidade do diretor responsável pelo tratamento de dados pessoais.

COMENTÁRIO: Quanto ao tratamento de dados pessoais no setor privado, inicia o Anteprojeto manifestando-se no sentido de que apenas empresas que contem com mais de 200 (duzentos) empregados deverão apontar diretor responsável pelo tratamento dos dados.

Não se entende a razão da estipulação desse valor, que deve ser alterado para abarcar, pelo menos, as empresas com atuação em âmbito eletrônico, independentemente do número de colaboradores, tendo em vista a grande possibilidade de perda das informações por elas tratadas, ainda que as menores não precisem ter empregado destacado especificamente para tal mister.

Chama-se atenção para a ligação direta da pessoa ou do departamento designado junto à Autoridade de Garantia como forma de garantir um canal efetivo de comunicação e *compliance* com as regras impostas por esta entidade.

Deve-se atentar também para a inclusão dessas responsabilidades nos Regulamentos Internos de Segurança da Informação – RISI e Termos de Uso de Segurança da Informação – TUSI da empresa, a fim de que ela também se resguarde quanto às funções do gestor do banco de dados.

CAPÍTULO XI TRANSFERÊNCIA INTERNACIONAL DE DADOS

Art. 35. A transferência internacional de dados pessoais somente é permitida para países que proporcionem um nível de proteção de dados equiparável ao da presente lei, salvo as seguintes exceções:

I - quando o titular tiver manifestado o próprio consentimento livre, expresso e informado para a transferência;

II - quando for necessária para a execução de obrigações derivadas de um contrato do qual o titular for parte;

III - quando for necessária para a garantia de um interesse público relevante previsto em lei;

IV – quando for necessária para a cooperação internacional entre órgãos públicos de inteligência e de investigação, de acordo com os instrumentos de direito internacional a que o Brasil se vincule;

V - quando for necessária para a defesa de um direito em juízo, se os dados forem transferidos exclusivamente para esta finalidade e pelo período de tempo necessário;

VI - quando for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro, se o titular não puder fornecer o próprio consentimento por impossibilidade física, por incapacidade de agir ou de compreender.

Art. 36. A Autoridade de Garantia reconhecerá o caráter adequado do nível de proteção de dados do país de destino levando em conta a legislação em vigor neste país e as demais circunstâncias relativas à transferência de dados.

Parágrafo único. Para os fins do previsto no caput, a Autoridade considerará a natureza dos dados, as normas gerais e setoriais presentes em seu ordenamento, a observância dos princípios de proteção de dados e das medidas de segurança previstas.

COMENTÁRIO: O art. 35 aborda a relevante questão da transferência internacional de dados. Em primeiro lugar, importante observar a previsão do *caput* no sentido de que isso somente é permitido entre países que apresentem nível de proteção de dados equiparável ao da presente lei, cabendo à Autoridade de Garantia posicionar-se sobre tal, como se observa no art. 39, XI do Anteprojeto. As exceções a necessidade de proporcionalidade entre os tratamento encontram fundamento no exposto nos incisos seguintes.

O inc. I expõe que caso o titular dos dados anua expressamente pela transferência internacional dos seus dados este procedimento é possível sem a intervenção da Autoridade de Garantia. Todavia, recaímos na mesma discussão sobre a transparência imprimida aos procedimentos de anuência (opt-in). Advogamos pela necessidade de provisão em apartada e expressa no caso de transferência internacional de dados.

O inc. IV traz em si a atual realidade de cooperação internacional para fins de investigação, algo imprescindível em face da natureza transnacional dos ilícitos praticados por organizações criminosas ou através de meios eletrônicos, que se aproveitam da ausência de fronteiras para perpetrar seus danos. Todavia, não podemos mitigar a aplicação do devido processo legal também nesses casos.

O inc. V é de extrema importância levando-se em consideração o próprio art. 3º da presente lei e o princípio da ubiquidade praticado por empresas que se utilizam de sistemas de computação em nuvem. O judiciário pátrio tem enfrentado diversos casos onde o fornecimento de dados para fins de defesa de direitos em juízo são negados por estes se encontrarem em outros países, mesmo quando as responsáveis por estes dados detém representantes em solo brasileiro.

O art. 36 dispõe como deve ser realizada essa comparação para fins de adequação, levando em conta não só a legislação em vigor, mas também

outras circunstâncias sobre transferência de dados, conforme descrito no parágrafo único do dispositivo. O norte para poder se interpretar a norma alienígena são os princípios expostos na presente lei.

Deve-se atentar, entretanto, para eventual burocratização excessiva dessa constatação de conformidade de tratamento internacional, o que pode inviabilizar a troca de informações, no caso de demora excessiva. A depender do tempo que se leve, pode-se estar diante de situações de grande gravidade que podem vir a ficar impunes.

Art. 37. A Autoridade de Garantia poderá autorizar uma transferência ou série de transferências para um país estrangeiro que não disponha de um nível adequado de proteção quando o responsável pelo tratamento ofereça garantias suficientes em relação à proteção da privacidade dos titulares, às medidas de segurança adotadas e a possibilidade do exercício dos direitos dispostos nesta lei.

Parágrafo único. A transferência de dados pessoais ao exterior, neste caso, somente poderá ocorrer após a autorização expressa da Autoridade de Garantia.

COMENTÁRIO: O artigo 37 traz previsões de situações em que, mesmo não estando atendidas as previsões de conformidade de tratamento aos dados pessoais do país para o qual eles serão enviados, ainda assim, essa troca possa ocorrer, desde que sejam dadas as mínimas garantias prescritas para tanto.

Apesar de trazer importantes previsões, entende-se que não há maiores razões para o tratamento dessas questões em tópico apartado, não havendo óbice algum a que eles constem de inciso ou de parágrafo único a ser acrescido ao artigo 35, a fim de melhor concentrar as exceções trazidas à regra expressa no *caput* do dispositivo.

TITULO II TUTELA ADMINISTRATIVA

CAPÍTULO I AUTORIDADE DE GARANTIA

Art. 38. É criado o Conselho Nacional de Proteção de Dados Pessoais, com autonomia administrativa, orçamentária e financeira, com a atribuição de atuar como Autoridade de Garantia quanto à proteção de dados pessoais, cuja estrutura e atribuições serão estabelecidas em legislação específica.

COMENTÁRIO: Apesar de diversos entendimentos em sentido contrário, entende-se ser salutar, em princípio, a criação de Conselho específico para tratar da proteção de dados pessoais, tendo em vista a necessidade de especialização daqueles que tratarão do tema. Sem dúvida, as organizações que hoje lidam com a temática o fazem de modo esparso e como atividade secundária, o que termina por representar certo amadorismo, bem como demora excessiva para responder questionamentos básicos.

A criação de entidade regulatória autônoma no âmbito da proteção de dados pessoais é natural em legislações estrangeiras, tendo por origem o Direito Italiano. A Europa detém entidades nacionais e supranacionais que têm por função primordial a conformidade das leis Estatais que introduzem em seus territórios as diretivas da comunidade.

Com a instituição de célula específica nesse sentido, espera-se que esses entraves referidos sejam solucionados, tendo-se célere e efetiva atuação do órgão, nos momento em que suscitado a se manifestar, atuando, de igual modo, em prestígio da segurança jurídica.

Art. 39. Compete ao Conselho Nacional de Proteção de Dados Pessoais:

I - zelar pela observância desta lei, de seu regulamento e do seu regimento interno;

II - planejar, elaborar, propor, coordenar e executar ações da política nacional de proteção de dados pessoais;

III - editar normas e provimentos sobre matérias de sua competência;

IV - aprovar seu regimento interno;

V - receber, analisar, avaliar e encaminhar consultas, denúncias, reclamações ou sugestões apresentadas por titulares de dados pessoais, entidades representativas ou pessoas jurídicas de direito público ou privado, referentes à proteção de dados pessoais, nos termos do regulamento;

VI – aplicar, de ofício ou a pedido de parte, conforme o caso, sanções, medidas corretivas e medidas preventivas que considere necessárias, na forma desta lei;

VII – criar, manter e publicar, para fins de transparência, um registro de bancos de dados pessoais de caráter de categorias e setores que considere relevantes, nos termos de regulamento;

VIII - verificar se os tratamentos respeitam as normas legais e os princípios gerais de proteção de dados;

IX - promover o conhecimento entre a população das normas que tratam da matéria e de suas finalidades, bem como das medidas de segurança de dados;

X - vetar, total ou parcialmente, o tratamento de dados ou prover seu bloqueio se o tratamento se torna ilícito ou inadequado, nos termos de regulamento;

XI - reconhecer o caráter adequado do nível de proteção de dados do país de destino no caso de transferência internacional de dados pessoais, bem como autorizar uma transferência ou série de transferências para países terceiros que não contem com este nível adequado;

XII – determinar ao responsável pelo tratamento de dados pessoais, quando necessário, a realização de estudo de impacto à privacidade, na forma de regulamento.

XIII - desenvolver outras atividades compatíveis com suas finalidades.

COMENTÁRIO: Como se observa, são amplas as possibilidade de atuação da Autoridade de Garantia, o que pode em casos específicos, trazer eventual esfera de conflito, com a coincidência de atribuições, fazendo-se necessária ter previsão sobre como esta procederá em casos como tais, a fim de se evitar a prorrogação por longo tempo de casos que se encaixem nessa situação.

Ainda, regulamento interno de funcionamento da Autoridade de Garantia deve ser publicado e tornado disponível ao cidadão para que este possa eficazmente utilizar os procedimentos administrativos oriundos de suas competências.

Art. 40. Os Estados, o Distrito Federal e os Municípios poderão criar suas próprias autoridades de proteção de dados pessoais, com competência concorrente e nas suas respectivas áreas de atuação administrativa.

COMENTÁRIO: O art. 40 se manifesta no sentido de que podem ser criadas diversas autoridades de proteção de dados pessoais, por parte dos Estados, do Distrito Federal e dos Municípios. Como se observa, não há maiores previsões acerca da forma de atuação de cada uma delas, limitando-se a prever que elas terão competência concorrente, mas com

base no princípio da simetria, devem ter competência e atuação semelhantes a Autoridade de Garantia de âmbito nacional, dentro de seus respectivos territórios. O presente artigo trata-se de uma faculdade dos entes federativos, mas tendo-se por foco que estas se subsumam a entidade de caráter nacional.

CAPÍTULO II SANÇÕES ADMINISTRATIVAS

Art. 41. Sem prejuízo das sanções civis e penais cabíveis e de outras sanções administrativas a serem definidas em normas específicas, as infrações das normas previstas nesta Lei ficam sujeitas, conforme o caso, às seguintes sanções administrativas:

I - multa;

II – bloqueio dos dados pessoais;

III – dissociação dos dados pessoais;

IV – cancelamento dos dados pessoais;

V – proibição do tratamento de dados sensíveis;

VI – suspensão temporária de atividade; e

VII – proibição de funcionamento do banco de dados.

§ 1º As sanções previstas neste artigo serão aplicadas pela Autoridade de Garantia, no âmbito de sua atribuição, podendo ser aplicadas cumulativamente, inclusive por medida cautelar, antecedente ou incidente de procedimento administrativo.

§2º As condições e procedimentos para a aplicação das sanções previstas, que devem ser graduadas em razão da gravidade, extensão da violação, natureza dos direitos pessoais afetados, reincidência e dos prejuízos dela derivados, serão determinados por meio de regulamentação.

Art. 42. A multa será estipulada:

I - no caso de empresa, em até vinte por cento do valor do faturamento bruto no seu último exercício, excluídos os impostos;

II - No caso das demais pessoas físicas ou jurídicas de direito público ou privado, bem como quaisquer associações de entidades ou pessoas constituídas de fato ou de direito, ainda que temporariamente, com ou sem personalidade jurídica, não sendo possível utilizar-se o critério do valor do faturamento bruto, em montante não inferior a R$ 2.000,00 (dois mil reais) e não superior a R$ 6.000.000,00 (seis milhões de reais).

Parágrafo único. Em caso de reincidência, as multas cominadas serão aplicadas em dobro, não se aplicando, em tal hipótese, o limite máximo indicado no inciso II.

COMENTÁRIO: Importante observar que o Anteprojeto, conforme consta de seus arts. 41 e 42, não trouxe qualquer previsão de aplicação de penas em âmbito criminal, sequer de instituição de tipos penais, limitando-se a traçar consequências administrativas e cíveis do descumprimento das normas trazidas.

Entende-se que se trata de opção a ser prestigiada, deixando-se eventuais especificação de medidas criminais para diploma específico, havendo, inclusive, o Projeto de Lei sobre Crimes da Internet, que tramita no Congresso Nacional, desde o ano de 1999, devendo-se, caso necessário, aí serem incluídas eventuais suscitações em âmbito penal.

Outrossim, cumpre observar que a previsão dos inciso I e II do art. 42, de aplicação de multas, sem qualquer justificativa do modo como se dará essa gradação, não corresponde à melhor forma de ser analisada o instituto, devendo-se tomar por base as prescrições trazidas no art. 57 do Código de Defesa do Consumidor, que leva em conta a gravidade da infração, a vantagem auferida e a condição econômica da parte.

Por fim, no caso do parágrafo segundo, deve-se melhor determinar o que se entende por reincidência, especificando lapso temporal apto a configurar tal perspectiva.

Art. 43. Sem prejuízo das sanções cabíveis, a Autoridade de Garantia, atuando de ofício ou a pedido de parte, deverá impor, aos responsáveis que incorram em infração às normas desta lei, as medidas corretivas que considere necessárias para reverter os efeitos danosos que a conduta infratora tenha causado ou para evitar que esta se produza novamente no futuro, fixando o valor da multa diária pelo seu descumprimento.

§1º As decisões administrativas transitadas em julgado que apliquem medidas corretivas em favor do titular dos dados constituem título executivo extrajudicial.

§2º Sempre que as medidas corretivas se dirigirem a um titular específico, é deste a legitimidade para executar a decisão.

Art. 44. Em qualquer fase do processo administrativo é facultado à Autoridade de Garantia adotar medidas preventivas, de ofício ou a pedido de parte, quando houver indício ou fundado receio de que o representado, direta ou indiretamente, cause ou possa causar à coletividade lesão irreparável ou de difícil reparação no âmbito da proteção de dados pessoais, ou torne ineficaz o resultado final do processo, fixando o valor da multa diária pelo seu descumprimento.

COMENTÁRIO: Importante observar, também, a natureza regulatória e cautelar do Anteprojeto, especialmente as constante dos arts. 43 e 44, propondo medidas inibitórias e corretivas, visando adequar a atuação das partes.

TITULO III CÓDIGOS DE BOAS PRÁTICAS

Art. 45. Os responsáveis pelo tratamento de dados pessoais, individualmente ou através de organizações de classe, poderão formular códigos de boas práticas que estabeleçam as condições de organização, regime de funcionamento, procedimentos aplicáveis, normas de segurança, padrões técnicos, obrigações específicas para os diversos envolvidos no tratamento e no uso de dados pessoais e demais quesitos e garantias para as pessoas, com pleno respeito aos princípios e disposições da presente lei e demais normas referentes à proteção de dados.

§1º Os códigos de boas práticas vincularão os respectivos responsáveis pelo tratamento de dados e os membros de uma determinada classe profissional.

§2º A Autoridade de Garantia solicitará às respectivas organizações de classe a elaboração dos códigos de boas práticas quando julgar conveniente e poderá participar de sua elaboração.

§3º Entre outras categorias profissionais, a Autoridade de Garantia priorizará o fomento à elaboração de códigos de boas práticas em tema de:

I - vigilância e monitoramento;

II - publicidade e marketing direto;

III - bancos de dados de proteção ao crédito;

IV - seguros; e

V - demais matérias pertinentes.

§4º Os códigos de boas práticas serão depositados na Autoridade de Garantia, que poderá não aprová-los se estiverem em desconformidade com as disposições legais e regulamentares sobre a matéria, ao que seguirá uma solicitação para que sejam feitas as modificações necessárias e

indicadas.

§5º Os códigos de boas práticas serão disponibilizados publicamente e deverão ser atualizados sempre que se demonstrar necessário.

COMENTÁRIO: O art. 45 traz específica determinação acerca do que se deve atentar quando ao se elaborar aos Regulamentos Internos de Segurança da Informação – RISI e Termos de Uso de Segurança da Informação - TUSI, sendo importante a observação de que eles deverão ser depositados perante a Autoridade de Garantia, consoante expressa determinação do art. §4º, que poderá desaprová-los, e tornados públicos.

Por fim, necessário se faz que seja melhor traçada a quem caberá a publicidade do código de boas práticas, aludida no §5º, se à Autoridade ou à parte que elaborou o documento, mormente se levando em conta que se está diante de documento obrigatório.

TITULO IV DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 46. Os direitos previstos nesta lei não excluem outros, decorrentes de tratados ou convenções internacionais de que o Brasil seja signatário, da legislação interna ordinária, bem como de regulamentos expedidos pelas autoridades administrativas competentes.

COMENTÁRIO: Trata-se de medida salutar, que facilita, inclusive, a troca de informações com as demais nações, coadunando-se com os ideias que guiaram o espírito do legislador, estando em sintonia, também, com a Constituição Federal.

Art. 47. Ficam revogados os artigos de 2º, 3° e 4º da Lei 9.507, de 12 de novembro de 1997.

COMENTÁRIO: A revogação dos artigos 2º, 3º e 4º da Lei 9.507, que regula o direito de acesso a informações e disciplina o rito processual do *habeas data*, em princípio, não se apresenta como medida salutar, tendo em vista que, consoante se trouxe, no Anteprojeto não consta, com clareza, o modo como se fará para proceder à retificação ou retirada dos dados pessoais, no caso de necessidade. Diante disso, entende-se devem ser mantidos os dispositivos, salvo se forem tratados os temas aludidos.

Art. 48. Esta Lei entrará em vigor no prazo de 90 dias contados da data

da sua publicação.

COMENTÁRIO: O prazo de *vacatio legis* parece ser suficiente para que as partes afetadas pela lei se adequem às suas previsões, até mesmo se levando em conta o amplo debate público que vem sendo feito em torno da questão.

CONCLUSÃO

Como se teve oportunidade de traçar, em vias gerais, o texto do Anteprojeto de Leis sobre Proteção de Dados Pessoais encontra-se bem redigido, havendo poucas questões de modificação de redação a serem levantadas.

Existem, contudo, alguns pontos que precisam ser melhor aclarados, a fim de que as disposições se adéquem melhor à realidade hoje enfrentada por todos que lidam com questões jurídicas derivadas da utilização dos mecanismos de tecnologia, quer sejam advogados, membros da Magistratura, do Ministério Público, Delegados de Polícia, Peritos, dentre outros.

Apenas reforçando alguns pontos principais que foram enfocados, traz-se o que diz respeito à falta de períodos mínimos para tratamento de dados pessoais (art. 30), sugerindo-se o prazo máximo de 180 (cento e oitenta dias), compatibilizando-se com o prazo trazido no art. 14 do Marco Civil da Internet.

Outrossim, não deve prosperar a distinção trazida sobre documentos eletrônicos e "texto escrito", como se observa ao longo dos arts. 9º; 13, VII; 15, §3º; 25, parágrafo único, dentre outros. Como já se teve a oportunidade de traçar, inúmeros diplomas nacionais, como a Medida Provisória que instituiu a Infraestrutura de Chaves Públicas Brasileiras (2.200-2/2001), a Lei do Processo Eletrônico (11.419/2006), já abordam a questão.

Ademais, o Projeto 166/2010, que trata da criação de novo diploma em âmbito cível tratou de disponibilizar seção exclusiva para tratar do tema, não se devendo dar continuidade à distinção aqui trazida, o que representa retrocesso que não se coaduna com a *ratio* e com o *occasio legis.*

Ademais, necessário se faz que bastante atenção seja dada ao tema, tendo em vista a crescente importância que vem sendo dada ao tema, bem como

as graves consequências de que vem sendo vítima a sociedade e os cidadãos, em razão do mal tratamento dos dados pessoais, ainda mais valor deve ser depositado no estudo dessa norma.

Espera-se que o trâmite dela no Congresso Nacional não seja burocratizado e demorado a ponto de tornar sem efetividade as prescrições trazidas pela norma, levando-se em consideração a velocidade do avanço tecnológico, de tão fundamentais que são para a continuidade da elevação das práticas levadas a efeito em ambiente virtual, enfocando-se a segurança jurídica, tão almejada por todos.

ENCERRAMENTO

Sendo o que tínhamos a comentar, ficamos a disposição para eventuais comentários, críticas e sugestões, como também contribuições adicionais ao tema de proteção de dados pessoais.

Renato Leite Monteiro
OAB/CE nº 20.068

Caio César Carvalho Lima
OAB/CE nº 23.903