

Anteprojeto de Lei para a Proteção de Dados Pessoais

Dispõe sobre o tratamento de dados pessoais para proteger a personalidade e a dignidade da pessoa natural

A PRESIDENTA DA REPÚBLICA

Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Comentário inicial: Ressalta-se que essa legislação que tem como objetivo a proteção dos dados pessoais e privacidade, já existente na Europa, inédita no arcabouço legal pátrio. Nessa iniciativa de consulta à sociedade, importante que tal legislação deve focar no estabelecimento de princípios, fundamentos e direitos. No apanhado do Anteprojeto, verifica-se o excessivo detalhamento operacional o que ensejaria numa demasiada burocracia no processo de tratamento dos dados o que poderá inviabilizar a oferta para grande quantidade de serviços. Dessa forma, deveria o legislador secundar o detalhamento em regulamentação posterior, na medida em que a lei amadureça no ordenamento e da real necessidade da intervenção para correção de deturpações que coloquem em risco as premissas e objetivos a serem alcançados por essa lei.

Por derradeiro, cabe salientar que tal lei não se restringe aos dados pessoais armazenados e tratados em ambiente eletrônico (internet). As demais mídias e veículos os quais envolvam armazenamento, tratamento, uso de dados pessoais estão também abrangidas por essa lei.

CAPÍTULO I – DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, com o objetivo de proteger os direitos fundamentais de liberdade, intimidade e privacidade da pessoa natural.

Art. 2º Esta Lei aplica-se a qualquer operação de tratamento realizada por meio total ou parcialmente automatizado, por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do país de sua sede e do país onde esteja localizado o banco de dados, desde que:

I – a operação de tratamento seja realizada no território nacional; ou

II – os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

Modificação: Nova redação do inciso II – os dados pessoais objeto do tratamento tenham sido coletados no território nacional, independente do local de armazenamento.

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

Modificação: § 1º Consideram-se coletados no território nacional quaisquer dados pessoais armazenados no Brasil; aqueles disponibilizados pelo titular, quando esse se encontrar em território brasileiro no momento da coleta; e aqueles disponibilizados pelo titular, quando esse se encontrar fora do território brasileiro, à pessoa jurídica com sede no país.

Justificativa: Alcança também os dados pessoais disponibilizados fora do território brasileiro, mas armazenados por pessoa jurídica situada no país.

§ 2º Esta Lei não se aplica aos tratamentos de dados:

I – realizados por pessoa natural para fins exclusivamente pessoais; ou

II – realizados para fins exclusivamente jornalísticos.

Inclusão de inciso: III – realizados em grandes massas de dados integrados, parcial ou inteiramente anonimizados.

Justificativa: A inclusão do inciso III (dados anônimos) entre as exceções, como uma técnica fundamental de apoio à tomada de decisão, inclusive em políticas públicas, e em setores como gerenciamento de trânsito e combate a epidemias, e que frequentemente utiliza procedimentos de anonimização dos dados.

Inclusão: IV - às informações, dados ou bancos de dados sujeitos a sigilo profissional ou legal, que permanecerão imunes a qualquer tipo de monitoramento ou tratamento por parte de terceiros estranhos ao titular ou ao profissional legítimo detentor.

Justificativa: manutenção da confidencialidade de dados protegidos pelo sigilo profissional

§ 3º É vedado aos órgãos públicos e entidades públicas efetuar a transferência de dados pessoais constantes de bases de dados que administram ou a que tenham acesso no exercício de suas competências legais para entidades privadas, exceto em casos de execução terceirizada ou mediante concessão e permissão de atividade pública que o exija e exclusivamente para fim específico e determinado.

Art. 3º As empresas públicas e sociedades de economia mista que atuem em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.

Parágrafo único. As empresas públicas e sociedades de economia mista, quando estiverem operacionalizando políticas públicas e não estiverem atuando em regime de concorrência, terão o mesmo tratamento dispensado aos órgãos e entidades públicas, nos termos dessa Lei.

Art. 4º Os tratamentos de dados pessoais para fins exclusivos de segurança pública, defesa, segurança do Estado, ou atividades de investigação e repressão de infrações penais, serão regidos por legislação específica, observados os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

Parágrafo único. É vedado o tratamento dos dados a que se refere o caput por pessoa de direito privado, salvo em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico ao órgão competente.

Comentário: Antes de se definir qual será o órgão competente a fiscalizar o cumprimento da lei, é necessário que se atenha a algumas premissas dentre elas: agir de forma imparcial e independente; possuir capacidade e composição técnica; não vir a aumentar a carga burocrática nos procedimentos e exigências administrativas, dificultando o dia-a-dia das empresas e cidadãos; que o conjunto excessivo de processos administrativos não venha a resultar em dificuldade de cumprimento dos operadores do tratamento de dados, ensejando conseqüentemente em penalizações, multas, etc.

Art. 5º Para os fins desta Lei, considera-se:

I – dado pessoal: dado relacionado à pessoa natural identificada ou identificável, inclusive a partir de números identificativos, dados locacionais ou identificadores eletrônicos;

II – tratamento: conjunto de ações referentes a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, transporte, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, bloqueio ou fornecimento a terceiros de dados pessoais, por comunicação, interconexão, transferência, difusão ou extração;

III – dados sensíveis: dados pessoais que revelem a origem racial ou étnica, as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, bem como dados genéticos;

IV – 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 para identificar o referido titular;

V – banco de dados: conjunto estruturado de dados pessoais, localizado em um ou em vários locais, em suporte eletrônico ou físico;

VI – titular: a pessoa natural a quem se referem os dados pessoais objeto de tratamento;

VII – consentimento: manifestação livre, expressa, específica e informada pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

VIII – responsável: a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

IX – operador: a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do responsável;

X – comunicação de dados: transferência de dados pessoais a um ou mais sujeitos determinados diversos do seu titular, sob qualquer forma;

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

XII – difusão: transferência de dados pessoais a um ou mais sujeitos indeterminados, diversos do seu titular, sob qualquer forma;

XIII – transferência internacional de dados: transferência de dados pessoais para um país estrangeiro;

XIV – 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;

XV – bloqueio: guarda do dado pessoal ou do banco de dados com a suspensão temporária de qualquer operação de tratamento;

XVI – cancelamento: eliminação de dados ou conjunto de dados armazenados em banco de dados, seja qual for o procedimento empregado;

XVII – uso compartilhado de dados: a comunicação, a difusão, a transferência internacional, a interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos, no cumprimento de suas competências legais, ou entre órgãos e entidades públicos e entes privados, com autorização específica, para uma ou mais modalidades de tratamento delegados por esses entes públicos; e

XVIII – encarregado: pessoa natural, indicada pelo responsável, que atua como canal de comunicação perante os titulares e o órgão competente.

Comentário: Antes de se definir qual será o órgão competente a fiscalizar o cumprimento da lei, é necessário que se atenha a algumas premissas dentre elas: agir de forma imparcial e independente; possuir capacidade e composição técnica; não vir a aumentar a carga burocrática nos procedimentos e exigências administrativas, dificultando o dia-a-dia das empresas e cidadãos; que o conjunto excessivo de processos administrativos não venha a resultar em dificuldade de cumprimento dos operadores do tratamento de dados, ensejando consequentemente em penalizações, multas, etc.

Art. 6º As atividades de tratamento de dados pessoais deverão atender aos seguintes princípios gerais:

I – princípio da finalidade, pelo qual o tratamento deve ser realizado com finalidades legítimas, específicas, explícitas e conhecidas pelo titular;

II – princípio da adequação, pelo qual o tratamento deve ser compatível com as finalidades almejadas e com as legítimas expectativas do titular, de acordo com o contexto do tratamento;

III – princípio da necessidade, pelo qual o tratamento deve se limitar ao mínimo necessário para a realização das finalidades almejadas, abrangendo dados pertinentes, proporcionais e não excessivos;

IV – princípio do livre acesso, pelo qual deve ser garantida consulta facilitada e gratuita pelos titulares sobre as modalidades de tratamento e sobre a integralidade dos seus dados pessoais;

V – princípio da qualidade dos dados, pelo qual devem ser garantidas a exatidão, a clareza e a atualização dos dados, de acordo com a periodicidade necessária para o cumprimento da finalidade de seu tratamento;

VI – princípio da transparência, pelo qual devem ser garantidas aos titulares informações claras e adequadas sobre a realização do tratamento;

VII – princípio da segurança, pelo qual devem ser utilizadas medidas técnicas e administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII – princípio da prevenção, pelo qual devem ser adotadas medidas capazes de prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; e

IX – princípio da não discriminação, pelo qual o tratamento não pode ser realizado para fins discriminatórios.

§ 1º Os órgãos públicos darão publicidade às suas atividades de tratamento de dados por meio de informações claras, precisas e atualizadas em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos, respeitando o princípio da transparência disposto no inciso VI.

§ 2º O uso compartilhado de dados pessoais deve atender a finalidade específica de execução de políticas públicas e atribuição legal pelos órgãos e entidades públicas, respeitando o princípio da finalidade, adequação e necessidade dispostos nos incisos I, II e III.

CAPÍTULO II – REQUISITOS PARA O TRATAMENTO DE DADOS PESSOAIS

Seção I – Consentimento

Comentário: Observamos que a lei contém definições muito estritas e inflexíveis sobre consentimento, e requer o cumprimento de certos requerimentos que, se mantidos como propostos neste texto, podem causar um impacto significativo na forma como os produtos, serviços e sistemas são projetados e oferecidos, assim como engessar a inovação, novos produtos e serviços que careçam do uso de dados.

A Lei não permite que o consentimento seja inferido a partir do contexto em que um serviço está sendo utilizado – por exemplo, ao prosseguir com a utilização de um serviço, o consumidor está concordando em fornecer seus dados para os propósitos previamente designados, a menos que o consumidor indique explicitamente que não deseja fornecer tais dados para um dado fim.

Por outro lado, a necessidade de consentimento explícito, quando combinada com o requerimento de prover informação completa, pode levar a uma sobrecarga de informação e escolhas, o que, por sua vez, levaria a uma cultura de consentimento. Nessa cultura, indivíduos fatigados do assunto adotam um de dois comportamentos: desistência do uso do serviço ou consentimento desinformado. No primeiro caso, cria-se um efeito econômico adverso; no segundo caso, o propósito original (decisão informada) não é alcançado.

Os requerimentos de aviso e consentimento explícito também podem levar a um redesenho em larga escala dos processos técnicos e comerciais por meio dos quais os dados são obtidos e utilizados, incluindo contratos, termos e condições, registros online, sistemas de relacionamento com o cliente. As implicações e custos associados a essas mudanças podem ter custos altíssimos para a indústria, e até inviabilizar do negócio empresas de pequeno porte que atuam no setor.

Finalmente, os requerimentos excessivos podem levar a constantes pedidos de autorização explícita, o que pode impedir que se obtenha dados que hoje são fundamentais para desenvolvimento de produto, marketing, e outras áreas que visam a oferecer melhores produtos e serviços para o consumidor.

Art. 7º O tratamento de dados pessoais somente é permitido após o consentimento livre, expresso, específico e informado do titular, salvo o disposto no art. 11.

§1º O consentimento para o tratamento de dados pessoais não pode ser condição para o fornecimento de produto ou serviço ou para o exercício de direito, salvo em hipóteses em que os dados forem indispensáveis para a sua realização.

§2º É vedado o tratamento de dados pessoais cujo consentimento tenha sido obtido mediante erro, dolo, estado de necessidade ou coação.

§3º O consentimento deverá ser fornecido por escrito ou por outro meio que o certifique.

Modificação: §3º O consentimento deverá ser fornecido por escrito ou por qualquer outro meio em direito admitido..

Justificativa: incluiria, além da escrita, formas digitais de fornecer o consentimento.

§4º O consentimento deverá ser fornecido de forma destacada das demais cláusulas contratuais.

§5º O consentimento deverá se referir a finalidades determinadas, sendo nulas as autorizações genéricas para o tratamento de dados pessoais.

§6º O consentimento pode ser revogado a qualquer momento, sem ônus para o titular.

Modificação: §6º O consentimento pode ser revogado a qualquer momento, sem ônus para o titular, sendo seus efeitos validos a partir da revogação, ressalvados sempre os direitos de terceiros de boa-fé.

Justificativa: garantia e segurança dos direitos de terceiros de boa-fé

§7º São nulas as disposições que estabeleçam ao titular obrigações iníquas, abusivas, que o coloquem em desvantagem exagerada, ou que sejam incompatíveis com a boa-fé ou a equidade.

§8º Cabe ao responsável o ônus da prova de que o consentimento do titular foi obtido em conformidade com o disposto nesta Lei.

Art. 8º O titular de dados pessoais com idade entre doze e dezoito anos idade poderá fornecer consentimento para tratamento que respeite sua condição peculiar de pessoa em desenvolvimento, ressalvada a possibilidade de revogação do consentimento pelos pais ou responsáveis legais, no seu melhor interesse.

Art. 9º No caso do titular de dados pessoais com idade até doze anos incompletos, o consentimento será fornecido pelos pais ou responsáveis legais, devendo o tratamento respeitar sua condição peculiar de pessoa em desenvolvimento.

Art. 10º No momento do fornecimento do consentimento, o titular será informado de forma clara, adequada e ostensiva sobre os seguintes elementos:

I – finalidade específica do tratamento;

Modificação: alterar para “finalidades específicas”

Justificativa: o consentimento poderá ser dado para mais de uma finalidade específica, respeitando .

II – forma e duração do tratamento;

Exclusão: excluir o inciso II do art. 10º

Justificativa: As finalidades e a duração já são informações suficientes para possibilitar ao usuário a tomada de decisão do consentimento ou não. A forma de tratamento poderá burocratizar o processo de tratamento.

III – identificação do responsável;

IV – informações de contato do responsável;

V – sujeitos ou categorias de sujeitos para os quais os dados podem ser comunicados, bem como âmbito de difusão;

Exclusão: excluir inciso V do art. 10º

Justificativa: Conforme exposto pelo grupo, impossibilidade operacional de se aplicar.

VI – responsabilidades dos agentes que realizarão o tratamento; e

VII – direitos do titular, com menção explícita a:

a) possibilidade de não fornecer o consentimento, com explicação sobre as consequências da negativa, observado o disposto no § 1º do art. 6º;

b) possibilidade de acessar os dados, retificá-los ou revogar o consentimento, por procedimento gratuito e facilitado; e

c) possibilidade de denunciar ao órgão competente o descumprimento de disposições desta Lei.

Comentário: Antes de se definir qual será o órgão competente a fiscalizar o cumprimento da lei, é necessário que se atenha a algumas premissas dentre elas: agir de forma imparcial e independente; possuir capacidade e composição técnica; não vir a aumentar a carga burocrática nos procedimentos e exigências administrativas, dificultando o dia-a-dia das empresas e cidadãos; que o conjunto excessivo de processos administrativos não venha a resultar em dificuldade de cumprimento dos operadores do tratamento de dados, ensejando consequentemente em penalizações, multas, etc.

§ 1º Considera-se nulo o consentimento caso as informações tenham conteúdo enganoso ou não tenham sido apresentadas de forma clara, adequada e ostensiva.

§ 3º Em caso de alteração de informação referida no inciso IV do caput, o responsável deverá comunicar ao titular as informações de contato atualizadas.

§ 4º Nas atividades que importem em coleta continuada de dados pessoais, o titular deverá ser informado regularmente sobre a continuidade dessa coleta de dados, nos termos definidos pelo órgão competente.

Comentário: Antes de se definir qual será o órgão competente a fiscalizar o cumprimento da lei, é necessário que se atenha a algumas premissas dentre elas: agir de forma imparcial e independente; possuir capacidade e composição técnica; não vir a aumentar a carga burocrática nos procedimentos e exigências administrativas, dificultando o dia-a-dia das empresas e cidadãos; que o conjunto excessivo de processos administrativos não venha a resultar em dificuldade de cumprimento dos operadores do tratamento de dados, ensejando consequentemente em penalizações, multas, etc.

Art. 11. O consentimento será dispensado quando os dados forem de acesso público irrestrito ou quando o tratamento for indispensável para:

I – cumprimento de uma obrigação legal pelo responsável;

II – tratamento e uso compartilhado de dados relativos ao exercício de direitos ou deveres previstos em leis ou regulamentos pela administração pública;

Modificação: excluir o termo tratamento

Justificativa: A dispensa do consentimento já é para o tratamento dos dados.

III – execução de procedimentos pré-contratuais ou obrigações relacionados a um contrato do qual é parte o titular, observado o disposto no § 1º do art. 6º;

IV – realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a dissociação dos dados pessoais;

V – exercício regular de direitos em processo judicial ou administrativo;

Modificação: excluir o termo “administrativo” e substituir por “ou quando permitido em lei”

Justificativa: só é admitida a quebra de sigilo em processo judicial. Há situações em que a lei permite que, p. ex., Delegados de Polícia podem requerer informações, dispensada a ordem judicial.

VI – proteção da vida ou da incolumidade física do titular ou de terceiro;

VII – tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias.

Inclusão do inciso VIII com a seguinte redação:

VIII - atender a interesse legítimo do responsável pelo tratamento de dados ou terceiros a quem os dados forem comunicados.

Justificativa: Incluir outra exceção à exigência de consentimento que é o tratamento de dados sempre houver "interesse legítimo". Este "interesse legítimo" é um dos pressupostos do tratamento de dados previstos na Diretiva de Proteção de Dados da União Europeia.

O "interesse legítimo" terá que ser: (a) um interesse legítimo do responsável ou de um terceiro a quem sejam fornecidos os dados (por exemplo, no caso de o titular deixar de pagar determinada prestação a um banco e o banco fornece os seus dados pessoais a uma empresa de cobrança para obter o pagamento da dívida pelo titular dos dados, embora o titular não tenha consentido), (b) esta exceção do interesse legítimo tem que respeitar os princípios de proteção de dados (princípio da qualidade dos dados e o princípio da necessidade e adequação, i.e., os dados têm que estar atualizados, e apenas serão transmitidos os dados necessários para a finalidade).

§ 1º Nas hipóteses de dispensa de consentimento, os dados devem ser tratados exclusivamente para as finalidades previstas e pelo menor período de tempo possível, conforme os princípios gerais dispostos nesta Lei, garantidos os direitos do titular.

§ 2º Nos casos de aplicação do disposto nos incisos I e II, será dada publicidade a esses casos, nos termos do parágrafo 1º do art. 6º.

§ 3º No caso de descumprimento do disposto no §2º, o operador ou o responsável pelo tratamento de dados poderá ser responsabilizado.

Inclusão do §4º com a seguinte redação:

§ 4º o tratamento de dados anônimos ou anonimizados.

Seção II – Dados Pessoais Sensíveis

Art. 12. É vedado o tratamento de dados pessoais sensíveis, salvo:

I – com fornecimento de consentimento especial pelo titular:

- a) mediante manifestação própria, distinta da manifestação de consentimento relativa a outros dados pessoais; e
- b) com informação prévia e específica sobre a natureza sensível dos dados a serem tratados, com alerta quanto aos riscos envolvidos no tratamento desta espécie de dados; ou

II – sem fornecimento de consentimento do titular, quando os dados forem de acesso público irrestrito, ou nas hipóteses em que for indispensável para:

- a) cumprimento de uma obrigação legal pelo responsável;
- b) **tratamento** e uso compartilhado de dados relativos ao exercício regular de direitos ou deveres previstos em leis ou regulamentos pela administração pública;

Modificação: excluir o termo "tratamento" da redação

Justificativa: A exceção à vedação do tratamento de dados sensíveis e a dispensa do consentimento especial já é para o tratamento dos dados, conforme caput do artigo.

c) realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a dissociação dos dados pessoais;

d) exercício regular de direitos em processo judicial **ou administrativo**;

Modificação: excluir o termo “ou administrativo” da redação.

Justificativa: somente nos processos judiciais.

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias.

§ 1º O disposto neste artigo aplica-se a qualquer tratamento capaz de revelar dados pessoais sensíveis.

§ 2º O tratamento de dados pessoais sensíveis não poderá ser realizado em detrimento do titular, ressalvado o disposto em legislação específica.

§ 3º Nos casos de aplicação do disposto nos itens ‘a’ e ‘b’ pelos órgãos e entidades públicas será dada publicidade à referida dispensa de consentimento, nos termos do §1o do art. 6o.

Art. 13. Órgão competente poderá estabelecer medidas adicionais de segurança e de proteção aos dados pessoais sensíveis, que deverão ser adotadas pelo responsável ou por outros agentes do tratamento.

§ 1º A realização de determinadas modalidades de tratamento de dados pessoais sensíveis poderá ser condicionada à autorização prévia de órgão competente, nos termos do regulamento.

Comentário: Antes de se definir qual será o órgão competente a fiscalizar o cumprimento da lei, é necessário que se atenha a algumas premissas dentre elas: agir de forma imparcial e independente; possuir capacidade e composição técnica; não vir a aumentar a carga burocrática nos procedimentos e exigências administrativas, dificultando o dia-a-dia das empresas e cidadãos; que o conjunto excessivo de processos administrativos não venha a resultar em dificuldade de cumprimento dos operadores do tratamento de dados, ensejando consequentemente em penalizações, multas, etc.

Justificativa: A lei já prevê consentimento prévio e especial do titular para tratamento dessa modalidade de dados pessoais.

§ 2º O tratamento de dados pessoais biométricos será disciplinado por órgão competente, que disporá sobre hipóteses em que dados biométricos serão considerados dados pessoais sensíveis.

Comentário: Antes de se definir qual será o órgão competente a fiscalizar o cumprimento da lei, é necessário que se atenha a algumas premissas dentre elas: agir de forma imparcial e independente; possuir capacidade e composição técnica; não vir a aumentar a carga burocrática nos procedimentos e exigências administrativas, dificultando o dia-a-dia das empresas e cidadãos; que o conjunto excessivo de processos administrativos não venha a resultar em dificuldade de cumprimento dos operadores do tratamento de dados, ensejando consequentemente em penalizações, multas, etc.

Seção III – Término do Tratamento

Art. 14. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

I – verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes para o alcance da finalidade específica almejada;

II - fim do período de tratamento;

III – comunicação do titular; ou

IV – determinação de órgão competente quando houver violação de dispositivo legal ou regulamentar.

Parágrafo único. Órgão competente estabelecerá períodos máximos para o tratamento de dados pessoais, ressalvado o disposto em legislação específica.

Comentário: Antes de se definir qual será o órgão competente a fiscalizar o cumprimento da lei, é necessário que se atenha a algumas premissas dentre elas: agir de forma imparcial e independente; possuir capacidade e composição técnica; não vir a aumentar a carga burocrática nos procedimentos e exigências administrativas, dificultando o dia-a-dia das empresas e cidadãos; que o conjunto excessivo de

processos administrativos não venha a resultar em dificuldade de cumprimento dos operadores do tratamento de dados, ensejando conseqüentemente em penalizações, multas, etc.

Art. 15. Os dados pessoais serão cancelados após o término de seu tratamento, autorizada a conservação para as seguintes finalidades:

I – cumprimento de obrigação legal pelo responsável;

II – pesquisa histórica, científica ou estatística, garantida, sempre que possível, a dissociação dos dados pessoais; ou

III – cessão a terceiros, nos termos desta Lei.

Parágrafo único. Órgão competente poderá estabelecer hipóteses específicas de conservação de dados pessoais, garantidos os direitos do titular, ressalvado o disposto em legislação específica.

Exclusão: do art. 14 e 15

Justificativa: Proposta a exclusão dos artigos. Após o término da relação contratual, é muitas vezes necessário conservar os dados pessoais, para resguardar direitos daquele que faz o tratamento dos dados, nas hipóteses de ações judiciais onde muitas vezes o ônus da prova é dele, bem como a fim de se verificar informações e evitar, p. ex., casos de fraudes de terceiros.

CAPÍTULO III – DIREITOS DO TITULAR

Art. 16. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais, garantidos os direitos fundamentais de liberdade, intimidade e privacidade, nos termos desta Lei.

Art. 17. O titular dos dados pessoais tem direito a obter:

I – confirmação da existência de tratamento de seus dados;

II – acesso aos dados;

III – correção de dados incompletos, inexatos ou desatualizados; e

IV – dissociação, bloqueio ou cancelamento de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei.

§1º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, alegando descumprimento ao disposto nesta Lei.

Exclusão: do § 1º

Justificativa: Uma vez discutidas e definidas as hipóteses de dispensa de consentimento e incluídas na Lei, é um contrassenso se abrir a possibilidade do titular questionar a sua aplicação. O texto do parágrafo é confuso

§ 2º Os direitos previstos neste artigo serão exercidos mediante requerimento do titular a um dos agentes de tratamento, que adotará imediata providência para seu atendimento.

§ 3º Em caso de impossibilidade de adoção imediata da providência de que trata o §2º, o responsável enviará ao titular, em até sete dias a partir da data do recebimento da comunicação, resposta em que poderá:

I – comunicar que não é agente de tratamento dos dados; ou

II – indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

Excluir: § 3º e incisos

§ 4º A providência de que trata o § 2º será realizada sem ônus para o titular.

Excluir: § 4º

§ 5º O responsável deverá informar aos terceiros a quem os dados tenham sido comunicados sobre a realização de correção, cancelamento, dissociação ou bloqueio dos dados, para que repitam idêntico procedimento.

Art. 18. A confirmação de existência ou o acesso a dados pessoais serão providenciados, a critério do titular:

I – em formato simplificado, imediatamente; ou

II – por meio de declaração clara e completa, que indique a origem dos dados, data de registro, critérios utilizados e finalidade do tratamento, fornecida no prazo de até sete dias, a contarem do momento do requerimento do titular.

§ 1º Os dados pessoais serão armazenados em formato que permita o exercício do direito de acesso.

§ 2º As informações e dados poderão ser fornecidos, a critério do titular:

I – por meio eletrônico, seguro e idôneo para tal fim; ou

II – sob a forma impressa, situação em que poderá ser cobrado exclusivamente o valor necessário ao ressarcimento do custo dos serviços e dos materiais utilizados.

§ 3º O titular poderá solicitar cópia eletrônica integral dos seus dados pessoais em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento, sempre que o banco de dados estiver em suporte eletrônico.

§ 4º Órgão competente poderá dispor sobre os formatos em que serão fornecidas as informações e os dados ao titular.

Exclusão: do artigo 18

Justificativa: Já há previsão no Código de Direitos do Consumidor (CDC), no artigo 43 as providências previstas no artigo 18.

Art. 19. O titular dos dados tem direito a solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive as decisões destinadas a definir o seu perfil ou avaliar aspectos de sua personalidade.

§ 1º O responsável deverá fornecer, sempre que solicitadas, informações adequadas a respeito dos critérios e procedimentos utilizados para a decisão automatizada.

§ 2º Ficam ressalvados os tratamentos de dados pessoais necessários ao cumprimento de obrigação legal.

Exclusão: do artigo 19

Justificativa: Mais um condicionante que estabelece obrigação operacional ao responsável e que é bastante discutível. O responsável deve ter o diretivo e a liberdade de avaliar os resultados do tratamento dos dados pessoais do titular, para seu uso interno, da forma como ele julgar mais adequada para si e para a destinação e finalidade que o tratamento dos dados tem.

Art. 20. Os dados pessoais referentes a exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

Art. 21. A defesa dos interesses e direitos dos titulares de dados poderá ser exercida em juízo individual ou coletivamente, na forma do disposto na Lei no 9.507, de 12 de novembro de 1997, nos arts. 81 e 82 da Lei no 8.078, de 11 de setembro de 1990, na Lei no 7.347, de 24 de julho de 1985, e nos demais instrumentos de tutela individual e coletiva.

Art. 22. Nos casos de comunicação ou interconexão de dados pessoais, o cessionário ficará sujeito às mesmas obrigações legais e regulamentares do cedente, com quem terá responsabilidade solidária pelos danos eventualmente causados.

Parágrafo único. A responsabilidade solidária não se aplica aos casos de comunicação ou interconexão realizadas no exercício dos deveres de que trata a Lei no 12.527, de 18 de novembro de 2011, relativos à garantia do acesso a informações públicas.

Art. 23. A comunicação ou interconexão de dados pessoais entre pessoas de direito privado dependerá de consentimento livre, expresso, específico e informado, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

Exclusão: do artigo 23

Justificativa: Artigo 10º já deixa claro que no momento do consentimento o usuário deve ser informado sobre sujeitos ou categorias de sujeitos para os quais os dados podem ser divulgados ou fornecidos a terceiros.

Art. 24. A comunicação ou interconexão de dados pessoais entre pessoa jurídica de direito público e pessoa de direito privado dependerá de consentimento livre, expresso, específico e informado do titular, salvo:

I – nas hipóteses de dispensa do consentimento previstas nesta Lei;

II – nos casos de uso compartilhado de dados previsto no inciso XVII do art. 5º, em que será dada publicidade nos termos do §1º do art. 6º; ou

III – quando houver prévia autorização de órgão competente, que avaliará o atendimento ao interesse público, a adequação e a necessidade da dispensa do consentimento.

Parágrafo único. A autorização prevista no inciso III do caput poderá ser condicionada:

I – à comunicação da interconexão aos titulares, nos termos do §1º do art. 6º;

II – ao oferecimento aos titulares de opção de cancelamento de seus dados; ou

III – ao cumprimento de obrigações complementares determinadas por órgão competente.

Art. 25. A comunicação ou interconexão entre órgãos e entidades de direito público será objeto de publicidade, nos termos do §1º do art. 6º, e obedecerá às regras gerais deste Capítulo.

Art. 26. O órgão competente poderá solicitar, a qualquer momento, aos órgãos e entidades públicos que realizem interconexão de dados e o uso compartilhado de dados pessoais, informe específico sobre o âmbito, natureza dos dados e demais detalhes do tratamento realizado, podendo emitir recomendações complementares para garantir o cumprimento desta Lei.

Art. 27. Órgão competente poderá estabelecer normas complementares para as atividades de comunicação e interconexão de dados pessoais.

Exclusão: dos artigos 24 ao 27

Justificativa: Para que a Lei possa efetivamente cumprir seu objetivo, o marco regulatório não deve criar distinção no tratamento das pessoas jurídicas de direito público e das pessoas jurídicas de direito privado. Assim, as pessoas jurídicas de direito público devem estar sujeitas às mesmas obrigações a que estão sujeitas as pessoas jurídicas de direito privado. Não deve, portanto, haver diferença da necessidade de consentimento livre, expresso, específico e informado consoante se trate de comunicação ou interconexão entre as pessoas jurídicas de direito público ou pessoas jurídicas de direito privado.

CAPÍTULO V – TRANSFERÊNCIA INTERNACIONAL DE DADOS

Comentário: O escopo extraterritorial da Lei é um aspecto importante para garantir a consistência e o equilíbrio dos requerimentos impostos às empresas de comunicações, a fim de, por sua vez, assegurar

aos consumidores um nível consistente de proteção, independente da localização da empresa. É também relevante garantir que o marco regulatório do Brasil também esteja consistente com outros importantes marcos regulatórios de impacto global, tais como a Regulação Geral de Proteção de Dados da União Europeia.

Os níveis de proteção de dados do país levem em consideração padrões internacionais de segurança e qualidade. Da mesma forma, a Lei deve estimular a utilização de mecanismos de autorregulação da indústria.

Art. 28. A transferência internacional de dados pessoais somente é permitida para países que proporcionem nível de proteção de dados pessoais equiparável ao desta Lei, ressalvadas as seguintes exceções:

I – quando a transferência for necessária para a cooperação judicial internacional entre órgãos públicos de inteligência e de investigação, de acordo com os instrumentos de direito internacional;

II – quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

III – quando órgão competente autorizar a transferência, nos termos de regulamento;

Comentário: Antes de se definir qual será o órgão competente a fiscalizar o cumprimento da lei, é necessário que se atenha a algumas premissas dentre elas: agir de forma imparcial e independente; possuir capacidade e composição técnica; não vir a aumentar a carga burocrática nos procedimentos e exigências administrativas, dificultando o dia-a-dia das empresas e cidadãos; que o conjunto excessivo de processos administrativos não venha a resultar em dificuldade de cumprimento dos operadores do tratamento de dados, ensejando consequentemente em penalizações, multas, etc.

IV – quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

V – quando a transferência for necessária para execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do §1º do art. 6º.

Parágrafo único. O nível de proteção de dados do país será avaliado por órgão competente, que levará em conta:

Comentário: Antes de se definir qual será o órgão competente a fiscalizar o cumprimento da lei, é necessário que se atenha a algumas premissas dentre elas: agir de forma imparcial e independente; possuir capacidade e composição técnica; não vir a aumentar a carga burocrática nos procedimentos e exigências administrativas, dificultando o dia-a-dia das empresas e cidadãos; que o conjunto excessivo de processos administrativos não venha a resultar em dificuldade de cumprimento dos operadores do tratamento de dados, ensejando consequentemente em penalizações, multas, etc.

I – normas gerais e setoriais da legislação em vigor no país de destino;

II – natureza dos dados;

III – observância dos princípios gerais de proteção de dados pessoais previstos nesta Lei;

IV – adoção de medidas de segurança previstas em regulamento; e

V – outras circunstâncias específicas relativas à transferência.

Modificação: Proposta de redação do Art. 28:

Art. 28. A transferência internacional de dados pessoais somente é permitida se o titular tiver manifestado previamente seu consentimento no momento do fornecimento do consentimento, ressalvadas as seguintes exceções:

I – quando a transferência for necessária para a cooperação judicial internacional entre órgãos públicos de inteligência e de investigação, de acordo com os instrumentos de direito internacional;

II – quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

III – quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

IV – quando a transferência for necessária para execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do §1º do art. 6º.

Justificativa: A transferência internacional deve ser autorizada pelo titular dos dados, cabendo ao titular decidir se concorda ou não com a transferência internacional e a transferência não pode estar relacionada a um fato que não esteja ao alcance e controle da entidade responsável, como a exigência de que o país de destino apresente lei com nível de proteção de dados pessoais equiparável ao desta Lei. Assim, sugerimos a supressão dos artigos 29 a 33

Art. 29. Nos casos de países que não proporcionem nível de proteção equiparável ao desta Lei, o consentimento de que trata o art. 7º será especial, fornecido:

I – mediante manifestação própria, distinta da manifestação de consentimento relativa a outras operações de tratamento; e

II – com informação prévia e específica sobre o caráter internacional da operação, com alerta quanto aos riscos envolvidos, de acordo com as circunstâncias de vulnerabilidade do país de destino.

Art. 30. A autorização referida no inciso III do caput do art. 28 será concedida quando o responsável pelo tratamento apresentar garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular, apresentadas em cláusulas contratuais aprovadas para uma transferência específica, em cláusulas contratuais-padrão ou em normas corporativas globais, nos termos do regulamento.

§ 1º Órgão competente poderá elaborar cláusulas contratuais-padrão e deverão observar os princípios gerais de proteção de dados e os direitos do titular, garantida a responsabilidade solidária, independente de culpa, de cedente e cessionário.

§ 2º Os responsáveis pelo tratamento que fizerem parte de um mesmo grupo econômico ou conglomerado multinacional poderão submeter normas corporativas globais à aprovação de órgão competente, obrigatórias para todas as empresas integrantes do grupo ou conglomerado, a fim de obter permissão para transferências internacionais de dados dentro do grupo ou conglomerado sem necessidade de autorizações específicas, observados os princípios gerais de proteção e os direitos do titular.

§ 3º Na análise de cláusulas contratuais ou de normas corporativas globais submetidas à aprovação de órgão competente, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento.

Art. 31. O cedente e o cessionário têm responsabilidade solidária pelo tratamento de dados realizado no exterior ou no território nacional, em qualquer hipótese, independente de culpa.

Art. 32. No caso de transferência internacional de dados de país estrangeiro para o Brasil, somente é permitido o seu tratamento no território nacional quando nas operações realizadas naquele país tiverem sido observadas suas normas relativas à obtenção de consentimento.

Art. 33. Órgão competente poderá estabelecer normas complementares que permitam identificar uma operação de tratamento como transferência internacional de dados pessoais.

Exclusão: dos art. 29 ao art. 33.

Justificativa: única redação pelo artigo 28.

CAPÍTULO VII – RESPONSABILIDADE DOS AGENTES

Seção I – Agentes do Tratamento e Ressarcimento de Danos

Art. 34. São agentes do tratamento de dados pessoais o responsável e o operador.

Art. 35. Todo aquele que, por meio do tratamento de dados pessoais, causar a outrem dano material ou moral, individual ou coletivo, é obrigado a ressarcir-lo.

§ 1º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação ou quando a produção de prova pelo titular resultar excessivamente onerosa;

§ 2º O responsável ou o operador podem deixar de ser responsabilizados se provarem que o fato que causou o dano não lhes é imputável.

Art. 36. A eventual dispensa da exigência do consentimento não desobriga os agentes do tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

Art. 37. As punições cabíveis no âmbito desta Lei serão aplicadas pessoalmente aos operadores e responsáveis de órgãos públicos que agirem de forma contrária a esta Lei, conforme disposto na Lei no 8.112, de 11 de dezembro de 1990 e na Lei no 8.429, de 2 de junho de 1992.

Art. 38. As competências e responsabilidades relativas à gestão de bases de dados nos órgãos e entidades públicos, bem como a responsabilidade pela prática de atos administrativos referentes a dados pessoais, serão definidas nos atos normativos que tratam da definição de suas competências.

Seção II – Responsável e Operador

Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo responsável, que verificará a observância das próprias instruções e das normas sobre a matéria.

§ 1º O responsável tem responsabilidade solidária quanto a todas as operações de tratamento realizadas pelo operador.

§ 2º Órgão competente poderá determinar ao responsável que elabore relatório de impacto à privacidade referente às suas operações de tratamento de dados, nos termos do regulamento.

Exclusão: do § 2º do art. 39

Justificativa: Entendemos que essa situação deve ser restrita a casos pontuais e especiais e que, por essa razão não deve estar expressa na Lei de forma genérica, bem como a proposta da não criação de órgão competente já justificada anteriormente.

Art. 40. O responsável ou o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, observado o disposto no art. 15.

Parágrafo único. Órgão competente poderá dispor sobre formato, estrutura e tempo de guarda do registro.

Excluir: o parágrafo único do art. 40.

Justificativa: A hipótese apresentada no artigo deve ser restrita a casos pontuais e especiais e que, por essa razão não deve estar expressa genericamente na Lei. A Lei, ao criar padrões de formatos poderia inviabilizar a prática. Os aspectos operacionais devem ser construídos gradativamente, conforme amadurecimento da lei na prática, motivados apenas por distorções que possam colocar em risco a consecução dos objetivos da Lei.

Seção III – Encarregado pelo Tratamento de Dados Pessoais

Art. 41. O responsável deverá indicar um encarregado pelo tratamento de dados pessoais.

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente de forma clara e objetiva, preferencialmente na página eletrônica do responsável na Internet.

§ 2º As atividades do encarregado consistem em:

I – receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II – receber comunicações do órgão competente e adotar providências;

Comentário: Antes de se definir qual será o órgão competente a fiscalizar o cumprimento da lei, é necessário que se atenha a algumas premissas dentre elas: agir de forma imparcial e independente; possuir capacidade e composição técnica; não vir a aumentar a carga burocrática nos procedimentos e exigências administrativas, dificultando o dia-a-dia das empresas e cidadãos; que o conjunto excessivo de processos administrativos não venha a resultar em dificuldade de cumprimento dos operadores do tratamento de dados, ensejando consequentemente em penalizações, multas, etc.

III – orientar os funcionários da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV – demais atribuições estabelecidas em normas complementares ou determinadas pelo responsável.

§ 3º Órgão competente estabelecerá normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de definição, conforme critérios de natureza ou porte da entidade, e volume de operações de tratamento de dados.

Comentário: Antes de se definir qual será o órgão competente a fiscalizar o cumprimento da lei, é necessário que se atenha a algumas premissas dentre elas: agir de forma imparcial e independente; possuir capacidade e composição técnica; não vir a aumentar a carga burocrática nos procedimentos e exigências administrativas, dificultando o dia-a-dia das empresas e cidadãos; que o conjunto excessivo de processos administrativos não venha a resultar em dificuldade de cumprimento dos operadores do tratamento de dados, ensejando consequentemente em penalizações, multas, etc.

Seção IV – Segurança e Sigilo dos Dados

Comentário: A Lei não define “incidente de segurança”, quais os dados e situações deveriam ser reportados ao eventual órgão competente, o qual em nossa proposta não seria necessário a sua criação. A comunicação imediata de ocorrências poderá criar pesados encargos para a indústria, tendo em vista que: o ato imediato pode comprometer ações de investigação e mitigação, pois nem toda ocorrência põe em risco a consumidores, e esse requerimento poderá levar a um volume alto de comunicações, o que, por sua vez, gerará trabalho excessivo para o setor público e divergir atenção de outros assuntos que poderiam ser mais importantes.

Art. 42. O operador deve adotar medidas de segurança técnicas e administrativas **constantemente atualizadas**, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação, difusão, ou qualquer forma de tratamento inadequado ou ilícito.

Modificação: excluir o termo “constantemente atualizadas” do caput do art. 42.

Justificativa: A lei deve exigir que as medidas adotadas sejam adequadas e proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais.

Parágrafo único. As medidas de segurança devem ser compatíveis com o atual estado da tecnologia, com a natureza dos dados e com as características específicas do tratamento, em particular no caso de dados sensíveis.

Art. 43. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se ao dever de sigilo em relação aos dados pessoais, mesmo após o seu término.

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.

Exclusão: art. 44

Comentário: Antes de se definir qual será o órgão competente a fiscalizar o cumprimento da lei, é necessário que se atenha a algumas premissas dentre elas: agir de forma imparcial e independente; possuir capacidade e composição técnica; não vir a aumentar a carga burocrática nos procedimentos e exigências administrativas, dificultando o dia-a-dia das empresas e cidadãos; que o conjunto excessivo de processos administrativos não venha a resultar em dificuldade de cumprimento dos operadores do tratamento de dados, ensejando consequentemente em penalizações, multas, etc.

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.

Exclusão: art. 45

Comentário: Antes de se definir qual será o órgão competente a fiscalizar o cumprimento da lei, é necessário que se atenha a algumas premissas dentre elas: agir de forma imparcial e independente; possuir capacidade e composição técnica; não vir a aumentar a carga burocrática nos procedimentos e exigências administrativas, dificultando o dia-a-dia das empresas e cidadãos; que o conjunto excessivo de processos administrativos não venha a resultar em dificuldade de cumprimento dos operadores do tratamento de dados, ensejando consequentemente em penalizações, multas, etc.

§ 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.

Comentário: Antes de se definir qual será o órgão competente a fiscalizar o cumprimento da lei, é necessário que se atenha a algumas premissas dentre elas: agir de forma imparcial e independente; possuir capacidade e composição técnica; não vir a aumentar a carga burocrática nos procedimentos e exigências administrativas, dificultando o dia-a-dia das empresas e cidadãos; que o conjunto excessivo de processos administrativos não venha a resultar em dificuldade de cumprimento dos operadores do tratamento de dados, ensejando consequentemente em penalizações, multas, etc.

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 normas complementares acerca de critérios e padrões mínimos de segurança, inclusive com base na evolução da tecnologia.

Comentário: Antes de se definir qual será o órgão competente a fiscalizar o cumprimento da lei, é necessário que se atenha a algumas premissas dentre elas: agir de forma imparcial e independente; possuir capacidade e composição técnica; não vir a aumentar a carga burocrática nos procedimentos e exigências administrativas, dificultando o dia-a-dia das empresas e cidadãos; que o conjunto excessivo de processos administrativos não venha a resultar em dificuldade de cumprimento dos operadores do tratamento de dados, ensejando consequentemente em penalizações, multas, etc.

Seção V – Boas Práticas

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.

Art. 49. O órgão competente estimulará a adoção de padrões técnicos para softwares e aplicações de Internet que facilitem a disposição dos titulares sobre seus dados pessoais, incluindo o direito ao não rastreamento.

Exclusão: Art. 48 e Art. 49

Justificativa: entendemos dispensável tal previsão na lei

CAPÍTULO VIII – SANÇÕES ADMINISTRATIVAS

Comentário: As sanções devem ser proporcionais ao risco que cada suposta violação possa causar aos consumidores. As sanções devem, ainda, ter como base os princípios da finalidade, motivação, razoabilidade, proporcionalidade, moralidade e interesse público, conforme se dispõe no caput do Artigo 2.º da Lei n.º 9784/1999, também previstos na Constituição Federal de 1988.

Art. 50. As infrações realizadas por pessoas jurídicas de direito privado às normas previstas nesta Lei ficam sujeitas às seguintes sanções administrativas aplicáveis por órgão competente:

Comentário: Antes de se definir qual será o órgão competente a fiscalizar o cumprimento da lei, é necessário que se atenha a algumas premissas dentre elas: agir de forma imparcial e independente; possuir capacidade e composição técnica; não vir a aumentar a carga burocrática nos procedimentos e exigências administrativas, dificultando o dia-a-dia das empresas e cidadãos; que o conjunto excessivo de processos administrativos não venha a resultar em dificuldade de cumprimento dos operadores do tratamento de dados, ensejando consequentemente em penalizações, multas, etc.

I – multa simples ou diária;

II – publicação da infração;

III – dissociação dos dados pessoais;

IV – bloqueio dos dados pessoais;

V – suspensão de operação de tratamento de dados pessoais, por prazo não superior a dois anos;

VI – cancelamento dos dados pessoais;

VII – proibição do tratamento de dados sensíveis, por prazo não superior a dez anos; e

VIII – proibição de funcionamento de banco de dados, por prazo não superior a dez anos.

§ 1º As sanções poderão ser aplicadas cumulativamente.

§ 2º Os procedimentos e critérios para a aplicação das sanções serão adequados em relação à gravidade e à extensão da infração, à natureza dos direitos pessoais afetados, à existência de reincidência, à situação econômica do infrator e aos prejuízos causados, nos termos do regulamento.

§ 3º Os prazos de proibição previstos nos incisos VII e VIII do caput poderão ser prorrogados pelo órgão competente, desde que verificada a omissão no cumprimento de suas determinações, a reincidência no cometimento de infrações ou a ausência de reparação integral de danos causados pela infração.

Comentário: Antes de se definir qual será o órgão competente a fiscalizar o cumprimento da lei, é necessário que se atenha a algumas premissas dentre elas: agir de forma imparcial e independente; possuir capacidade e composição técnica; não vir a aumentar a carga burocrática nos procedimentos e exigências administrativas, dificultando o dia-a-dia das empresas e cidadãos; que o conjunto excessivo de processos administrativos não venha a resultar em dificuldade de cumprimento dos operadores do tratamento de dados, ensejando consequentemente em penalizações, multas, etc.

§ 4º O disposto neste artigo não prejudica a aplicação de sanções administrativas, civis ou penais definidas em legislação específica.

§ 5º O disposto nos incisos III a VII poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei no 8.112, de 11 de dezembro de 1990 e na Lei no 8.429, de 2 de junho de 1992.

CAPÍTULO IX – DISPOSIÇÕES TRANSITÓRIAS E FINAIS

Art. 51. Órgão competente estabelecerá normas sobre adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, considerada a complexidade das operações de tratamento, a natureza dos dados e o porte do responsável.

Comentário: Antes de se definir qual será o órgão competente a fiscalizar o cumprimento da lei, é necessário que se atenha a algumas premissas dentre elas: agir de forma imparcial e independente; possuir capacidade e composição técnica; não vir a aumentar a carga burocrática nos procedimentos e exigências administrativas, dificultando o dia-a-dia das empresas e cidadãos; que o conjunto excessivo de processos administrativos não venha a resultar em dificuldade de cumprimento dos operadores do tratamento de dados, ensejando consequentemente em penalizações, multas, etc.

Art. 52. Esta Lei entrará em vigor no prazo de 120 (cento e vinte) dias contados da data da sua publicação.

Modificar: “120 (cento e vinte) dias” por “18 (dezoito) meses”.

Justificativa: Acreditamos que o prazo razoável para adaptação e aderência dos entes à legislação seria de 18 meses.

Brasília, de de 2015; 194º da Independência e 127º da República.