ANTEPROJETO DE LEI

Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural

A **PRESIDENTA DA REPÚBLICA** Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Art. 2º A disciplina da proteção de dados pessoais no Brasil tem como fundamento o respeito à privacidade, bem como:

I - a autodeterminação informativa;

II - a liberdade de expressão, comunicação e opinião;

III – a inviolabilidade da intimidade, vida privada, honra e imagem;

IV - o desenvolvimento econômico e tecnológico; e

V - a livre iniciativa, a livre concorrência e a defesa do consumidor.

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do país de sua sede ou do país onde estejam localizados os dados, desde que:

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

II – a atividade de tratamento tenha por objetivo a oferta ou fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou

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

Parágrafo único. Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

Art. 4º Esta Lei não se aplica ao tratamento de dados:

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

II – realizado para fins exclusivamente jornalísticos, artísticos, literários ou acadêmicos; ou

III - realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais.

§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, observados os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

§ 2º É vedado o tratamento dos dados a que se refere o inciso III 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.

§ 3º O órgão competente emitirá opiniões técnicas ou recomendações referentes às exceções previstas nos incisos II e III, bem como poderá solicitar aos responsáveis relatórios de impacto à privacidade.

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

I - dado pessoal: dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa;

II - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

III - dados sensíveis: dados pessoais sobre a origem racial ou étnica, as convicções religiosas, 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 ou biométricos;

IV - dados anonimizados: dados relativos a um titular que não possa ser identificado;

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 e inequívoca 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 - encarregado: pessoa natural, indicada pelo responsável, que atua como canal de comunicação perante os titulares e o órgão competente;

XI - transferência internacional de dados: transferência de dados pessoais para um país estrangeiro;

XII - anonimização: qualquer procedimento por meio do qual um dado deixa de poder ser associado, direta ou indiretamente, a um indivíduo;

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

XIV - eliminação: exclusão definitiva de dado ou de conjunto de dados armazenados em banco de dados, seja qual for o procedimento empregado; e

XV - uso compartilhado de dados: a comunicação, a difusão, a transferência internacional, a interconexão de dados pessoais ou o 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.

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I – finalidade: pelo qual o tratamento deve ser realizado para finalidades legítimas, específicas, explícitas e informadas ao titular;

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

III – necessidade: pelo qual o tratamento deve se limitar ao mínimo necessário para a realização das suas finalidades, abrangendo dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

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

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

VI – transparência: pelo qual devem ser garantidas aos titulares informações claras, adequadas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento;

VII – 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 – prevenção: pelo qual devem ser adotadas medidas capazes de prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; e

IX – não discriminação: pelo qual o tratamento não pode ser realizado para fins discriminatórios.

CAPÍTULO II

REQUISITOS PARA O TRATAMENTO DE DADOS PESSOAIS

Seção I

Requisitos para o tratamento

Art 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento pelo titular de consentimento livre e inequívoco;

II - para o cumprimento de uma obrigação legal pelo responsável;

III - pela administração pública, para o tratamento e uso compartilhado de dados relativos ao exercício de direitos ou deveres previstos em leis ou regulamentos;

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

V - quando necessário para a execução de um contrato ou de procedimentos preliminares relacionados a um contrato do qual é parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo judicial ou administrativo;

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;

IX – quando necessário para atender aos interesses legítimos do responsável, respeitados os interesses ou os direitos e liberdades fundamentais do titular.

§ 1º Nos casos de aplicação do disposto nos incisos II e III, o titular deverá ser informado do tratamento de seus dados.

§ 2º No caso de descumprimento do disposto no § 1º, o operador ou o responsável pelo tratamento de dados poderá ser responsabilizado.

§ 3º O tratamento de dados pessoais cujo acesso é público deve ser realizado de acordo com esta lei, considerando a finalidade, a boa-fé e o interesse público que justificou a sua disponibilização.

Art. 8º O titular deverá ter acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva sobre, entre outros:

I - finalidade específica do tratamento;

II - forma e duração do 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;

VI - responsabilidades dos agentes que realizarão o tratamento; e

VII - direitos do titular, com menção explícita a:

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

b) possibilidade de denunciar ao órgão competente o descumprimento de disposições desta Lei; e

c) possibilidade de não fornecer o consentimento, na hipótese em que o consentimento é requerido, mediante o fornecimento de informações sobre as consequências da negativa.

§ 1º Na hipótese em que o consentimento é requerido, este será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou não tenham sido apresentadas previamente de forma clara, adequada e ostensiva.

§ 2º Em caso de alteração de informação referida no inciso IV do caput, o responsável deverá comunicar ao titular as informações de contato atualizadas.

§ 3º Nas atividades que importem em coleta continuada de dados pessoais, o titular deverá ser informado periodicamente sobre as principais características do tratamento, nos termos definidos pelo órgão competente.

§ 4º Quando o consentimento para o tratamento de dados pessoais for condição para o fornecimento de produto ou serviço ou para o exercício de direito, o titular será informado com destaque sobre tal fato e sobre os meios pelos quais poderá exercer controle sobre o tratamento de seus dados.

§ 5º O órgão competente poderá dispor sobre os meios referidos no parágrafo anterior.

Art. 9º O consentimento previsto no art. 7º, I deverá ser livre e inequívoco e fornecido por escrito ou por qualquer outro meio que o certifique.

§ 1º Caso o consentimento seja fornecido por escrito, este deverá ser fornecido em cláusula destacada das demais cláusulas contratuais.

§ 2º Cabe ao responsável o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

§ 3º É vedado o tratamento de dados pessoais quando o consentimento tenha sido obtido mediante erro, dolo, coação, estado de perigo ou simulação.

§ 4º O consentimento deverá se referir a finalidades determinadas, sendo nulas as autorizações genéricas para o tratamento de dados pessoais.

§ 5º O consentimento pode ser revogado a qualquer momento, mediante manifestação expressa do titular.

§ 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 8º, o responsável deverá obter novo consentimento do titular, após destacar de forma específica o teor das alterações.

§ 7º O órgão competente poderá adequar os requisitos para o consentimento, considerando o contexto em que é fornecido e a natureza dos dados pessoais fornecidos.

Art. 10. O legítimo interesse do responsável somente poderá fundamentar um tratamento de dados pessoais, respeitados os direitos e liberdades fundamentais do titular, devendo ser necessário e baseado em uma situação concreta.

§ 1º O legítimo interesse deverá contemplar as legítimas expectativas do titular quanto ao tratamento de seus dados, de acordo com o disposto no art. 6º, II.

§ 2º O responsável deverá adotar medidas para garantir a transparência do tratamento de dados baseado no seu legítimo interesse, devendo fornecer aos titulares mecanismos eficazes para que possam manifestar sua oposição ao tratamento de dados pessoais.

§ 3º Quando o tratamento for baseado no legítimo interesse do responsável, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados, devendo ser anonimizados sempre que compatível com a finalidade do tratamento.

§ 4º O órgão competente poderá solicitar ao responsável relatório de impacto à privacidade quando o tratamento tiver como fundamento o seu interesse legítimo.

Art. 11. É vedado o tratamento de dados pessoais sensíveis, salvo:

I - com fornecimento de consentimento inequívoco, expresso e específico 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 seu tratamento.

II - sem fornecimento de consentimento do titular, 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;

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

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

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

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 de dados pessoais 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 O disposto no item 'c' do inciso II somente se aplicará caso as atividades descritas não estejam vinculadas a atividade comercial, de administração pública, investigação criminal ou inteligência, garantindo-se, sempre que possível, a anonimização dos dados pessoais.

§ 4º Nos casos de aplicação do disposto nos itens 'a' e 'b' do inciso II pelos órgãos e entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do art. 24.

Art. 12. O 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, ou solicitar a apresentação de relatório de impacto à privacidade.

Art 13. Os dados anonimizados serão considerados dados pessoais para os fins desta Lei quando o processo de anonimização ao qual foram submetidos for revertido ou quando, com esforços razoáveis, puder ser revertido.

§ 1º Poderão ser igualmente considerados como dados pessoais para os fins desta Lei os dados utilizados para a formação do perfil comportamental de uma determinada pessoa natural, ainda que não identificada.

§ 2º O órgão competente poderá dispor sobre padrões e técnicas utilizadas em processos de anonimização e realizar verificações acerca de sua segurança.

§ 3º O compartilhamento e o uso que se faz de dados anonimizados deve ser objeto de publicidade e de transparência, sem prejuízo do órgão competente poder solicitar ao responsável relatório de impacto à privacidade referente aos riscos de reversão do processo de anonimização e demais aspectos de seu tratamento.

Art. 14. O tratamento de dados pessoais de criança e pessoa absolutamente incapaz, nos termos da lei, somente pode ser realizado mediante consentimento dos responsáveis legais e no seu melhor interesse.

Parágrafo único. O tratamento de dados pessoais de adolescente e pessoa relativamente incapaz observará as seguintes condições:

I - autorização condicionada à supervisão, assistência ou anuência do responsável legal; e

II – respeito à sua condição pessoal, podendo os responsáveis legais revogar o consentimento para tratamento de dados pessoais a qualquer tempo.

Seção II – Término do Tratamento

Art. 15. 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, inclusive no exercício do seu direito de revogação do consentimento conforme disposto no art. 9, § 5º; ou

IV – determinação do órgão competente, quando houver violação da legislação em vigor a respeito.

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

Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, autorizada a conservação para as seguintes finalidades:

I - cumprimento de obrigação legal do responsável;

II – pesquisa histórica, científica ou estatística, garantida, quando possível, a anonimização dos dados pessoais; ou

III - transferência a terceiros, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei.

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

CAPÍTULO III

DIREITOS DO TITULAR

Art. 17. 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. 18. O titular dos dados pessoais tem direito a obter, em relação aos seus dados:

I - confirmação da existência de tratamento;

II - acesso aos dados;

III - correção de dados incompletos, inexatos ou desatualizados;

IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

V - portabilidade, mediante requisição, de seus dados pessoais a outro fornecedor de serviço ou produto;

VI - eliminação, a qualquer momento, de dados pessoais com cujo tratamento o titular tenha consentido; e

VII - aplicação das normas de defesa do consumidor, quando for o caso, na tutela da proteção de dados pessoais.

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

§ 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 do requerimento, resposta em que poderá:

I - comunicar que não é agente de tratamento dos dados, indicando, sempre que possível, quem o seja; ou

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

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

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

Art. 19. 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 contar da data do requerimento do titular.

§ 1º Os dados pessoais serão armazenados em formato que favoreça 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 forma impressa, situação em que poderá ser cobrado exclusivamente o valor necessário ao ressarcimento do custo dos serviços e dos materiais utilizados.

§ 3º Quando o tratamento tiver origem no consentimento do titular ou em um contrato, 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.

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

§ 5º O órgão competente poderá dispor de forma diferenciada acerca dos prazos dos incisos I e II do caput para setores específicos.

Art. 20. 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.

Parágrafo único. O responsável deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e procedimentos utilizados para a decisão automatizada, respeitado o segredo comercial e industrial.

Art. 21. Os dados pessoais referentes a exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

Art. 22. 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.

CAPITULO VI

Do Tratamento de Dados Pessoais pelo Poder Público

Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referenciadas no parágrafo único do art. 1º da Lei 12.527, de 18 de novembro de 2011, deverá ser realizado para o atendimento de sua finalidade pública, na persecução de um interesse público, tendo por objetivo a execução de competências legais ou o cumprimento de atribuição legal pelo serviço público.

Art. 24. Os órgãos do Poder Público darão publicidade às suas atividades de tratamento de dados pessoais 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 art 5º, VI desta Lei.

§ 1º Os órgãos do Poder Público que realizem operações de tratamento de dados pessoais deverão indicar um encarregado, nos termos do art. 40.

§ 2º O órgão competente poderá dispor sobre as formas pelas quais se dará a publicidade das operações de tratamento.

Art 25. As empresas públicas e sociedades de economia mista que atuem em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal, 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 do Poder Público, nos termos desse Capítulo.

Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e entidades públicas, respeitando os princípios da proteção de dados pessoais elencados no art. 6º desta Lei.

Parágrafo único. É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto em casos de execução descentralizada de atividade pública que o exija e exclusivamente para este fim específico e determinado, observado, ainda, o disposto na Lei nº 12.527, de 18 de novembro de 2011.

Art. 27. A comunicação e transferência de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informada ao órgão competente e dependerá de consentimento do titular, salvo:

I - nas hipóteses de dispensa do consentimento previstas nesta Lei; ou:

II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do art. 24.

Art. 28. A comunicação de dados pessoais entre órgãos e entidades de direito público será objeto de publicidade, nos termos art. 24.

Art. 29. O órgão competente poderá solicitar, a qualquer momento, às entidades do Poder Público que realizem operações de tratamento de dados pessoais, informe específico sobre o âmbito, natureza dos dados e demais detalhes do tratamento realizado, podendo emitir parecer técnico complementar para garantir o cumprimento desta Lei.

Art. 30. O órgão competente poderá estabelecer normas complementares para as atividades de comunicação de dados pessoais.

Seção II

Responsabilidade

Art. 31. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, o órgão competente poderá enviar informe com medidas cabíveis para fazer cessar a violação.

Parágrafo único. As punições cabíveis a agente público no âmbito desta Lei serão aplicadas pessoalmente aos operadores de órgãos públicos, 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. 32. O órgão competente poderá solicitar a agentes do poder público que publiquem relatórios de impacto de privacidade e sugerir adoção de padrões e boas práticas aos tratamentos de dados pessoais pelo poder público.

CAPÍTULO V

TRANSFERÊNCIA INTERNACIONAL DE DADOS

Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:

I - para países que proporcionem nível de proteção de dados pessoais ao menos equiparável ao desta Lei;

II - 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;

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

IV - quando o órgão competente autorizar a transferência;

V - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

VI - quando a transferência for necessária para execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do art. 24.

VII - quando o titular tiver fornecido o seu consentimento para a transferência, com informação prévia e específica sobre o caráter internacional da operação, com alerta quanto aos riscos envolvidos.

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

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.

Art. 34. A autorização referida no inciso IV do caput do art. 33 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 pelo órgão competente para uma transferência específica, em cláusulas contratuais padrão ou em normas corporativas globais, nos termos do regulamento.

§ 1º O órgão competente poderá elaborar cláusulas contratuais padrão ou homologar dispositivos constantes em documentos que fundamentem a transferência internacional de dados, que deverão observar os princípios gerais de proteção de dados e os direitos do titular, garantida a responsabilidade solidária do cedente e do cessionário, independentemente de culpa.

§ 2º Os responsáveis pelo tratamento que fizerem parte de um mesmo grupo econômico ou conglomerado multinacional poderão submeter normas corporativas globais à aprovação do 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, documentos ou de normas corporativas globais submetidas à aprovação do órgão competente, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento.

§ 4º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no caput serão, também, analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos §1° e §2° do artigo 45.

Art. 35. O cedente e o cessionário respondem solidária e objetivamente pelo tratamento de dados, independentemente do local onde estes se localizem, em qualquer hipótese.

CAPÍTULO VI – AGENTES DO TRATAMENTO DE DADOS PESSOAIS

Seção I – Responsável e Operador

Art. 36. São agentes do tratamento de dados pessoais o responsável e o operador.

Art. 37. O responsável e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem.

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

Art. 38. 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.

Art. 39. O 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.

Art. 40. A comunicação de dados pessoais entre responsáveis ou operadores de direito privado dependerá do consentimento do titular, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

Seção II – 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;

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

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

§ 3º O órgão competente poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e porte da entidade ou volume de operações de tratamento de dados.

Seção III – Responsabilidade e Ressarcimento de Danos

Art. 42. Todo aquele que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, é obrigado a repará-lo.

Parágrafo único. 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-lhe excessivamente onerosa.

Art. 43. 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. 44. Nos casos que envolvem a transferência 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 tratamento realizado 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.

CAPÍTULO VII - SEGURANÇA E BOAS PRÁTICAS

Seção I - Segurança e Sigilo de Dados

Art. 45. O operador deve adotar medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

§ 1º O órgão competente poderá dispor sobre padrões técnicos e organizacionais para tornar aplicável o disposto no caput, levando-se em consideração a natureza das informações tratadas, características específicas do tratamento e o estado atual da tecnologia, em particular no caso de dados sensíveis.

§ 2º As medidas de segurança deverão ser observadas desde a fase de concepção do produto ou serviço até a sua execução.

Art. 46. 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. 47. O responsável deverá comunicar ao órgão competente a ocorrência de qualquer incidente de segurança que possa acarretar risco ou prejuízo relevante aos titulares.

Parágrafo único. A comunicação será feita em prazo razoável e 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;

V - no caso da comunicação não ter sido imediata, os motivos da demora; e

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

Art. 48. O órgão competente verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao responsável a adoção de outras providências, tais como:

I - pronta comunicação aos titulares;

II - ampla divulgação do fato em meios de comunicação; e

III - medidas para reverter ou mitigar os efeitos do incidente.

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

§ 2º A pronta comunicação aos titulares afetados pelo incidente de segurança será obrigatória, independente de determinação do órgão competente, nos casos em que for possível identificar que o incidente coloque em risco a segurança pessoal dos titulares ou lhes possa causar danos.

Art. 49 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.

Seção II – Boas Práticas

Art. 50. 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 educativas, mecanismos internos de supervisão e outros aspectos relacionados ao tratamento de dados pessoais.

§ 1º Ao estabelecer regras de boas práticas, o responsável pelo tratamento e o operador levarão em consideração a natureza, escopo e finalidade do tratamento e dos dados, bem como a probabilidade e gravidade dos riscos de danos aos indivíduos.

§ 2º As regras de boas práticas disponibilizadas publicamente e atualizadas poderão ser reconhecidas e divulgadas pelo órgão competente.

Art. 51. O órgão competente estimulará a adoção de padrões técnicos que facilitem o controle dos titulares sobre seus dados pessoais.

CAPÍTULO VIII

FISCALIZAÇÃO

Seção I

Sanções Administrativas

Art. 52. As infrações realizadas por pessoas jurídicas de direito privado às normas previstas nesta Lei ficam sujeitas às seguintes sanções administrativas aplicáveis pelo órgão competente:

I - multa simples ou diária;

II - publicização da infração;

III - anonimização dos dados pessoais;

IV - bloqueio dos dados pessoais;

V - suspensão de operação de tratamento de dados pessoais;

VI - cancelamento dos dados pessoais;

VII - suspensão de funcionamento de banco de dados.

§ 1º As sanções serão aplicadas fundamentadamente, isolada ou cumulativamente, de acordo com as peculiaridades do caso concreto e com a gravidade e natureza das infrações, à natureza dos direitos pessoais afetados, à existência de reincidência, à situação econômica do infrator e aos prejuízos causados.

§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas em legislação específica.

§ 3º 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.

Seção II

Órgão Competente e Conselho Nacional de Proteção de Dados e da Privacidade

Art. 53. O órgão competente designado para zelar pela implementação e fiscalização da presente Lei terá as seguintes atribuições:

I – zelar pela proteção dos dados pessoais, nos termos da legislação;

II – elaborar diretrizes para uma Política Nacional de Proteção de Dados Pessoais e Privacidade;

III - promover entre a população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais, bem como das medidas de segurança;

IV – promover estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;

V - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais;

VI - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transacional;

VII - elaborar relatórios anuais acerca de suas atividades;

VIII – editar normas sobre proteção de dados pessoais e privacidade; e

IX - realizar demais ações dentro de sua esfera de competência, inclusive as previstas nesta Lei e em legislação.

Art. 54. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade contará com quinze representantes titulares e quinze suplentes designados pelo Ministro de Estado da Justiça, com mandato de dois anos, podendo ser renovado uma única vez por igual período, sendo:

I – sete representantes do Poder Executivo Federal, indicados por ato do Poder Executivo;

II - um representante indicado pela Câmara dos Deputados;

III - um representante indicado pelo Senado Federal;

IV – um representante indicado pelo Conselho Nacional de Justiça;

V – um representante indicado pelo Conselho Nacional do Ministério Público;

VI – um representante indicado pelo Comitê Gestor da Internet no Brasil;

VII – um representante da sociedade civil;

VIII- um representante da academia; e

IX - dois representantes do setor privado.

§ 1º A participação no Conselho Nacional será considerada atividade de relevante interesse público, não remunerada.

§ 2º Os representantes referidos no inciso II ao VI do caput e seus respectivos suplentes serão indicados pelos titulares dos respectivos órgãos e entidades.

§ 3º Os representantes referidos nos incisos VII a IX do caput e seus respectivos suplentes serão indicados, nos termos do regimento interno a ser aprovado posteriormente.

Art. 55. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade:

I - fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade;

II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade;

III - sugerir ações a serem realizadas pelo órgão competente;

IV - realizar estudos e debates sobre a proteção de dados pessoais e da privacidade; e

V - disseminar o conhecimento sobre proteção de dados pessoais e privacidade à população em geral.

CAPÍTULO IX

DISPOSIÇÕES TRANSITÓRIAS E FINAIS

Art. 56. Esta Lei entrará em vigor no prazo de 180 dias contados da data da sua publicação.

Parágrafo único: O 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 e a natureza dos dados.