



SENADO FEDERAL

PARECER Nº 129, DE 2018 – PLEN/SF

Redação final do Projeto de Lei da Câmara nº 53, de 2018 (nº 4.060, de 2012, na Casa de origem).

A **Comissão Diretora**, em **Plenário**, apresenta a redação final do Projeto de Lei da Câmara nº 53, de 2018 (nº 4.060, de 2012, na Casa de origem), que *dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014*, consolidando as emendas de redação aprovadas pelo Plenário.

Senado Federal, em 10 de julho de 2018.

JOÃO ALBERTO SOUZA, PRESIDENTE

ANTONIO CARLOS VALADARES, RELATOR

EDUARDO AMORIM

SÉRGIO PETECÃO

ANEXO DO PARECER N° 129, DE 2018 – PLEN/SF

Redação final do Projeto de Lei da Câmara nº 53, de 2018 (nº 4.060, de 2012, na Casa de origem).

Dispõe sobre o tratamento e a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

O CONGRESSO NACIONAL decreta:

CAPÍTULO I DISPOSIÇÕES PRELIMINARES

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

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

I – o respeito à privacidade;

II – a autodeterminação informativa;

III – a liberdade de expressão, de informação, de comunicação e de opinião;

IV – a inviolabilidade da intimidade, da honra e da imagem;

V – o desenvolvimento econômico e tecnológico e a inovação;

VI – a livre iniciativa, a livre concorrência e a defesa do consumidor;

VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

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 meio, 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 o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;

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

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

§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso III do *caput* do art. 4º desta Lei.

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

I – realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

II – realizado para fins exclusivamente:

- a) jornalísticos;
- b) artísticos;
- c) acadêmicos, aplicando-se a esta hipótese os arts. 13 e 17 desta Lei;
- d) de segurança pública;
- e) de defesa nacional;
- f) de segurança do Estado;
- g) de atividades de investigação e repressão de infrações penais;

III – provenientes de fora do território nacional e que:

a) não sejam objeto de comunicação ou de uso compartilhado com agentes de tratamento brasileiros;

b) sejam objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

§ 1º O tratamento de dados pessoais para as finalidades previstas nas alíneas “d” a “g” do inciso II do *caput* deste artigo observará as seguintes regras:

I – será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei;

II – não poderá ser realizado por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no inciso III deste § 1º;

III – em nenhum caso a totalidade dos dados pessoais do banco de dados poderá ser tratada por pessoa de direito privado.

§ 2º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes ao tratamento de dados pessoais para as finalidades previstas nas alíneas “d” a “g” do inciso

II do *caput* deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.

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

I – dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II – dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, saúde, vida sexual, genética ou biometria, quando vinculado a pessoa natural;

III – dado anonimizado: dado relativo a titular que não possa ser identificado, utilizando-se meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

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

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

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

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

VIII – encarregado: pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional;

IX – agentes de tratamento: o controlador e o operador;

X – autoridade nacional: órgão da administração pública indireta responsável pelo cumprimento desta Lei;

XI – órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;

XII – 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, controle, modificação, comunicação, transferência, difusão ou extração;

XIII – anonimização: processo em que um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, mediante utilização de meios técnicos razoáveis e disponíveis no momento do tratamento;

XIV – consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para finalidade determinada;

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

XVI – eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados;

XVII – transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

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

XIX – relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

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

I – finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com esses propósitos;

II – adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III – necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com a utilização de dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento;

IV – livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V – qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI – transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII – segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de eventos acidentais ou ilícitos de destruição, perda, alteração, comunicação ou difusão;

VIII – prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX – não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X – responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

CAPÍTULO II

DOS DIREITOS DO TITULAR

Art. 7º Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

Art. 8º O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

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 dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;

VI – eliminação dos dados tratados com o seu consentimento, exceto nas hipóteses previstas no art. 22 desta Lei;

VII – informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

VIII – informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX – revogação do consentimento, nos termos do § 5º do art. 14 desta Lei.

§ 1º O titular dos dados pessoais, em relação aos seus dados, tem o direito de peticionar contra o controlador perante a autoridade nacional.

§ 2º 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.

§ 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento, que deverá adotar as providências cabíveis.

§ 4º Em caso de impossibilidade de adoção imediata das providências referidas no § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:

I – comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente;

II – indicar as razões de fato ou de direito que impedem a adoção imediata das providências.

§ 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.

§ 6º A correção, a eliminação, a anonimização e o bloqueio de dados deverão ser imediatamente informados pelo controlador aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados, para que repitam idêntico procedimento.

§ 7º A portabilidade dos dados pessoais a que se refere o inciso V do *caput* deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.

§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os órgãos de defesa do consumidor.

Art. 9º Mediante requisição do titular, a confirmação da existência de tratamento será atestada, e o acesso aos dados pessoais será concedido:

I – em formato simplificado, imediatamente; ou

II – por meio de declaração clara e completa que indique a origem dos dados, a inexistência de registro e os critérios utilizados para o tratamento, bem como a sua finalidade, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado 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 os dados poderão ser fornecidos, a critério do titular:

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

II – sob forma impressa.

§ 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização posterior, inclusive em outras operações de tratamento.

§ 4º Para setores específicos, a autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do *caput* deste artigo.

Art. 10. O titular dos dados tem direito a solicitar revisão, por pessoa natural, de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive de decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

§ 2º Em caso de não fornecimento das informações referidas no § 1º baseado na observância de segredo comercial ou industrial, a autoridade nacional poderá realizar auditoria para verificar aspectos discriminatórios em tratamento automatizado de dados pessoais.

Art. 11. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

Art. 12. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, por meio dos instrumentos de tutela individual e coletiva.

CAPÍTULO III

DO TRATAMENTO DE DADOS PESSOAIS

Seção I

Dos Requisitos para o Tratamento de Dados Pessoais

Art. 13. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I – mediante o fornecimento de consentimento pelo titular;

II – para o cumprimento de obrigação legal ou regulatória pelo controlador;

III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV – para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

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

VI – para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

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

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

IX – quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;

X – para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

§ 1º Nos casos de aplicação do disposto nos incisos II e III do *caput* deste artigo e excetuadas as hipóteses previstas no art. 4º desta Lei, o titular será informado das hipóteses em que será admitido o tratamento de seus dados.

§ 2º A forma de disponibilização das informações previstas no § 1º e no inciso I do *caput* do art. 23 desta Lei poderá ser especificada pela autoridade nacional.

§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

§ 4º É dispensada a exigência do consentimento previsto no *caput* deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.

§ 5º O controlador que obteve o consentimento referido no inciso I do *caput* deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores

deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

Art. 14. O consentimento previsto no inciso I do art. 13 desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.

§ 2º Cabe ao controlador 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 mediante vício de consentimento.

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

§ 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do *caput* do art. 8º desta Lei.

§ 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 15 desta Lei, o controlador deverá informar, de forma específica e destacada, o seu teor ao titular, o qual, nos casos em que seu consentimento é exigido, poderá revogá-lo caso discorde da alteração.

Art. 15. O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

I – finalidade específica do tratamento;

II – forma e duração do tratamento, observados os segredos comercial e industrial;

III – identificação do controlador;

IV – informações de contato do controlador;

V – informações acerca do uso compartilhado de dados pelo controlador e a finalidade do compartilhamento;

VI – responsabilidades dos agentes que realizarão o tratamento; e

VII – direitos do titular, com menção explícita aos direitos contidos no art. 8º desta Lei.

§ 1º Na hipótese em que o consentimento for requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

§ 2º Na hipótese em que o consentimento for requerido, se houver mudança da finalidade para o tratamento de dados pessoais não compatível com o consentimento original,

o controlador deverá informar previamente o titular, o qual poderá revogar o consentimento, caso discorde das alterações.

§ 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 8º desta Lei.

Art. 16. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I – apoio e promoção de atividades do controlador;

II – proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Seção II

Do Tratamento de Dados Pessoais Sensíveis

Art. 17. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I – quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II – sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

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

f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 15 desta Lei e excetuado o caso em que prevaleçam direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

§ 2º Nos casos de aplicação do disposto nas alíneas “a” e “b” do inciso II do *caput* deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do *caput* do art. 23 desta Lei.

§ 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.

§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nos casos de portabilidade de dados quando consentido pelo titular.

Art. 18. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

§ 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

§ 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais, previsto no art. 58 desta Lei.

Art. 19. Na realização de estudos e pesquisas em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

§ 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o *caput* deste artigo em nenhuma hipótese poderá revelar dados pessoais.

§ 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no *caput* deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro.

§ 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.

§ 4º Para os efeitos deste artigo, a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Seção III Do Tratamento de Dados Pessoais de Crianças e de Adolescentes

Art. 20. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

§ 1º O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

§ 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 8º desta Lei.

§ 3º Poderão ser coletados dados pessoais de crianças e de adolescentes sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, caso em que serão utilizados uma única vez e sem armazenamento, ou para protegê-las, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.

§ 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

§ 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado por um dos pais ou pelo responsável legal pela criança ou adolescente, consideradas as tecnologias disponíveis.

§ 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físicomotoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança ou do adolescente.

Seção IV Do Término do Tratamento de Dados

Art. 21. 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 ao alcance da finalidade específica almejada;

II – fim do período de tratamento;

III – comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 14 desta Lei, resguardado o interesse público; ou

IV – determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

Art. 22. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

I – cumprimento de obrigação legal ou regulatória pelo controlador;

II – estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

III – transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou

IV – uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

CAPÍTULO IV DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

Seção I Das Regras

Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas nos incisos I e II do parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado no exercício de suas competências para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou para cumprir as atribuições legais do serviço público, desde que:

I – sejam informadas as hipóteses em que realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;

II – sejam protegidos e preservados dados pessoais de requerentes de acesso à informação, nos termos da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), vedado seu compartilhamento no âmbito do Poder Público e com pessoas jurídicas de direito privado;

III – seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais.

§ 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento.

§ 2º Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do *Habeas Data*), da Lei nº

9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo), e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

§ 3º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no *caput* deste artigo, nos termos desta Lei.

§ 4º Os órgãos notariais e de registro devem fornecer, por meio eletrônico, acesso aos dados à administração pública, para fins do disposto no *caput* deste artigo.

§ 5º O disposto nesta Lei não dispensa as pessoas jurídicas referidas no *caput* deste artigo de observar a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

Art. 24. As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado, nos termos desta Lei.

Parágrafo único. As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos deste Capítulo.

Art. 25. Os dados pessoais tratados pelo Poder Público deverão ser mantidos em formato interoperável e estruturados para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

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 pelas entidades públicas, respeitados os princípios de proteção de dados pessoais referidos no art. 6º desta Lei.

§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:

I – em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);

II – quando houver previsão legal, e a transferência for respaldada em contratos, convênios ou instrumentos congêneres;

III – nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.

§ 2º Os contratos, os convênios e os instrumentos congêneres referidos no inciso II do § 1º deste artigo deverão ser comunicados à autoridade nacional.

Art. 27. A comunicação de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado, bem como o uso compartilhado desses dados, serão informados à autoridade nacional e dependerão de consentimento do titular, exceto:

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

II – nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do *caput* do art. 23 desta Lei;

III – nos casos previstos nos incisos I, II e III do § 1º do art. 26 desta Lei.

Art. 28. A comunicação e o uso compartilhado de dados pessoais entre órgãos e entidades de direito público serão objeto de publicidade, nos termos do inciso I do *caput* do art. 23 desta Lei.

Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, às entidades do Poder Público, realização de operações de tratamento de dados pessoais, informe específico sobre o âmbito e a natureza dos dados e demais detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei.

Art. 30. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

Art. 31. A autoridade nacional poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais.

Seção II Da Responsabilidade

Art. 32. Quando houver violação a esta Lei em decorrência do tratamento de dados pessoais pelo Poder Público, a autoridade nacional poderá enviar ao responsável informe com medidas cabíveis para fazer cessá-la.

CAPÍTULO V DA TRANSFERÊNCIA INTERNACIONAL DE DADOS

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

I – para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;

II – quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:

- a) cláusulas contratuais específicas para determinada transferência;
- b) cláusulas-padrão contratuais;
- c) normas corporativas globais;
- d) selos, certificados e códigos de conduta regularmente emitidos;

III – quando necessária à cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

IV – quando necessária à proteção da vida ou da incolumidade física do titular ou de terceiro;

V – quando autorizada pela autoridade nacional;

VI – quando resultar em compromisso assumido em acordo de cooperação internacional;

VII – quando necessária à execução de política pública ou ao cumprimento de atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do *caput* do art. 23 desta Lei;

VIII – quando o titular tiver fornecido consentimento específico e em destaque, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades;

IX – quando necessária para atender as hipóteses previstas nos incisos II, V e VI do art. 13 desta Lei.

Art. 34. Para os fins do inciso I do art. 33 desta Lei, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), no âmbito de suas competências legais, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.

Parágrafo único. Na avaliação referida no *caput*, a autoridade nacional levará em consideração:

I – as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;

II – a natureza dos dados;

III – a observância aos princípios gerais de proteção de dados pessoais e aos direitos dos titulares previstos nesta Lei;

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

V – a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais;

VI – outras circunstâncias específicas relativas à transferência de dados.

Art. 35. A autoridade nacional definirá o conteúdo das garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados nas formas previstas nas alíneas do inciso II do *caput* do art. 33 desta Lei e poderá requerer informações suplementares e realizar diligências de verificação quanto às operações de tratamento, quando necessário.

§ 1º A autoridade nacional poderá designar organismos de certificação para as atividades referidas no *caput* deste artigo, nos termos definidos em regulamento.

§ 2º Os organismos de certificação referidos no § 1º permanecerão sob fiscalização da autoridade nacional, que poderá revisar ou anular os atos por eles praticados, em caso de desconformidade com esta Lei.

§ 3º As garantias referidas no *caput* deste artigo serão analisadas de acordo com medidas de segurança técnicas e administrativas adotadas pelo operador, de acordo com o previsto no art. 46 desta Lei.

Art. 36. Qualquer alteração nas garantias referidas no inciso II do art. 33 desta Lei deverá ser comunicada à autoridade nacional.

CAPÍTULO VI

DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS

Seção I

Do Controlador e do Operador

Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

Parágrafo único. O relatório referido no *caput* deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Art. 39. O operador deverá realizar o tratamento de dados de acordo com as instruções fornecidas pelo controlador, que verificará a observância dessas instruções e das normas sobre a matéria.

Art. 40. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados, segurança e tempo de guarda dos registros, observados os princípios da necessidade e da transparência.

Seção II

Do Encarregado pelo Tratamento de Dados Pessoais

Art. 41. O controlador deverá indicar 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 no sítio eletrônico do controlador.

§ 2º As atividades do encarregado consistem em:

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

II – receber comunicações da autoridade nacional e adotar providências;

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

IV – executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

§ 3º A autoridade nacional poderá estabelecer normas complementares sobre o encarregado, inclusive sua definição, suas atribuições e hipóteses de dispensa de sua indicação, conforme a natureza e o porte da entidade e o volume de operações de tratamento de dados.

Seção III Da Responsabilidade e do Ressarcimento de Danos

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:

I – o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipóteses em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

II – os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

§ 2º 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, houver hipossuficiência para fins de produção de prova ou a produção de prova pelo titular resultar-lhe excessivamente onerosa.

§ 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do *caput* deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.

§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:

I – que não realizaram o tratamento de dados pessoais que lhes é atribuído;

II – que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou

III – que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dos dados pode esperar, consideradas as circunstâncias relevantes, entre as quais:

I – o modo pelo qual o tratamento é realizado;

II – o resultado e os riscos que razoavelmente se esperam do tratamento;

III – as técnicas de tratamento disponíveis à época em que foi realizado.

Parágrafo único. Respondem pelos danos decorrentes da violação da segurança dos dados o controlador e o operador que, ao deixarem de adotar as medidas de segurança previstas no art. 46 desta Lei, derem causa ao dano.

Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.

CAPÍTULO VII

DA SEGURANÇA E DAS BOAS PRÁTICAS

Seção I

Da Segurança e do Sigilo de Dados

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de eventos acidentais ou ilícitos de destruição, perda, alteração, comunicação ou difusão ou qualquer outra ocorrência decorrente de tratamento inadequado ou ilícito.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para fins do disposto no *caput* deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no *caput* do art. 6º desta Lei.

§ 2º As medidas de que trata o *caput* deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Art. 47. O agente de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir, mesmo após o seu término, a segurança da informação prevista nesta Lei em relação aos dados pessoais.

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I – a descrição da natureza dos dados pessoais afetados;

II – as informações sobre os titulares envolvidos;

III – as medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV – os riscos relacionados ao incidente;

V – os motivos da demora, no caso de a comunicação não ter sido imediata; e

VI – as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente.

§ 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:

I – ampla divulgação do fato em meios de comunicação; e

II – medidas para reverter ou mitigar os efeitos do incidente.

§ 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiro não autorizado a acessá-los.

Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Seção II Das Boas Práticas e da Governança

Art. 50. Os controladores e os operadores, individualmente ou por meio de associações, poderão, no âmbito de suas competências, formular, para os diversos envolvidos no tratamento de dados pessoais, regras de boas práticas e de governança que estabeleçam condições de organização, regime de funcionamento, procedimentos – inclusive de reclamações e de petições de titulares –, normas de segurança, padrões técnicos, obrigações específicas, ações educativas, mecanismos internos de supervisão e de mitigação de riscos e outras medidas relacionadas ao tratamento.

§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração a natureza, o escopo e a finalidade do tratamento e dos dados, bem como a gravidade dos riscos e a probabilidade dos benefícios decorrentes do tratamento de dados do titular.

§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do *caput* do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

I – implementar programa de governança em privacidade que, no mínimo:

a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente que lhe assegure mecanismos de participação;

f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

g) conte com planos de resposta a incidentes e remediação; e

h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

II – demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.

§ 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.

CAPÍTULO VIII DA FISCALIZAÇÃO

Seção I Das Sanções Administrativas

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, estão sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

I – advertência, com indicação de prazo para adoção de medidas corretivas;

II – multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III – multa diária, observado o limite total a que se refere o inciso II;

IV – publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V – bloqueio dos dados pessoais a que se refere a infração até a regularização da atividade de tratamento pelo controlador;

VI – eliminação dos dados pessoais a que se refere a infração;

VII – suspensão parcial ou total do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período até a regularização da atividade de tratamento pelo controlador;

VIII – suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;

IX – proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

§ 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto, observada a proporcionalidade entre a gravidade da falta e a intensidade da sanção, e considerados os seguintes parâmetros e critérios:

I – a gravidade e a natureza das infrações e dos direitos pessoais afetados;

II – a boa-fé do infrator;

III – a vantagem auferida ou pretendida pelo infrator;

IV – a condição econômica do infrator;

V – a reincidência;

VI – a extensão do dano;

VII – a cooperação do infrator;

VIII – a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;

IX – a adoção de política de boas práticas e governança;

X – a pronta adoção de medidas corretivas.

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

§ 3º O disposto nos incisos I, IV, V, VI, VII, VIII e IX do *caput* deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal), na Lei nº 8.429, de 2 de junho de 1992 (Lei de Improbidade Administrativa), e na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

§ 4º No cálculo do valor da multa de que trata o inciso II do *caput* deste artigo, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea.

Art. 53. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa.

§ 1º As metodologias a que se refere o *caput* deste artigo devem ser previamente publicadas, para ciência dos agentes de tratamento, e devem apresentar objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa, que deverão conter fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos nesta Lei.

§ 2º O regulamento de sanções e metodologias correspondentes deve estabelecer as circunstâncias e as condições para a adoção de multa simples ou diária.

Art. 54. O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional.

Parágrafo único. A intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento.

CAPÍTULO IX

DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE

Seção I

Da Autoridade Nacional de Proteção de Dados (ANPD)

Art. 55. É criada a Autoridade Nacional de Proteção de Dados (ANPD), integrante da administração pública federal indireta, submetida a regime autárquico especial e vinculada ao Ministério da Justiça.

§ 1º A ANPD deverá observar as disposições da Lei nº 9.986, de 18 de julho de 2000.

§ 2º A ANPD será composta do Conselho Diretor, como órgão máximo, e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, além das unidades especializadas para a aplicação desta Lei.

§ 3º A natureza de autarquia especial conferida à ANPD é caracterizada por independência administrativa, ausência de subordinação hierárquica, mandato fixo e estabilidade de seus dirigentes e autonomia financeira.

§ 4º O regulamento e a estrutura organizacional da ANPD serão aprovados por decreto do Presidente da República.

§ 5º O Conselho Diretor será composto de 3 (três) conselheiros e decidirá por maioria.

§ 6º O mandato dos membros do Conselho Diretor será de 4 (quatro) anos.

§ 7º Os mandatos dos primeiros membros do Conselho Diretor serão de 3 (três), 4 (quatro) e 5 (cinco) anos, conforme estabelecido no decreto de nomeação.

§ 8º É vedado a ex-conselheiro utilizar informações privilegiadas obtidas em decorrência do cargo exercido, sob pena de incorrer em improbidade administrativa.

Art. 56. A ANPD terá as seguintes atribuições:

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

II – zelar pela observância dos segredos comercial e industrial em ponderação com a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei;

III – elaborar diretrizes para Política Nacional de Proteção de Dados Pessoais e da Privacidade;

IV – fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;

V – atender petições de titular contra controlador;

VI – disseminar o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança à população;

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

VIII – estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, devendo esses padrões levar em consideração as especificidades das atividades e o porte dos responsáveis;

IX – promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;

X – dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, observado o respeito aos segredos comercial e industrial;

XI – solicitar, a qualquer momento, às entidades do Poder Público que realizem operações de tratamento de dados pessoais, informe específico sobre o âmbito e a natureza dos dados e os demais detalhes do tratamento realizado, podendo emitir parecer técnico complementar para garantir o cumprimento desta Lei;

XII – elaborar relatórios de gestão anuais acerca de suas atividades;

XIII – editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, assim como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco para a garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei;

XIV – ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante, assim como prestar contas sobre suas atividades e planejamento;

XV – arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do *caput* deste artigo, o detalhamento de suas receitas e despesas; e

XVI – realizar ou determinar a realização de auditorias, no âmbito da atividade de fiscalização, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluindo o Poder Público.

§ 1º Ao impor condicionamentos administrativos ao tratamento de dados pessoais por agente de tratamento privado, sejam eles limites, encargos ou sujeições, a ANPD deve observar a exigência de mínima intervenção, assegurados os fundamentos, os princípios e os direitos previstos no art. 170 da Constituição Federal e nesta Lei.

§ 2º Os regulamentos e normas editados pela ANPD devem necessariamente ser precedidos de consulta e audiência públicas, bem como de análises de impacto regulatório.

Art. 57. Constituem receitas da ANPD:

I – o produto da execução da sua dívida ativa;

II – as dotações consignadas no orçamento geral da União, os créditos especiais, os créditos adicionais, as transferências e os repasses que lhe forem conferidos;

III – as doações, os legados, as subvenções e outros recursos que lhe forem destinados;

IV – os valores auferidos na venda ou aluguel de bens móveis e imóveis de sua propriedade;

V – os valores auferidos em aplicações no mercado financeiro das receitas previstas neste artigo;

VI – o produto da cobrança de emolumentos por serviços prestados;

VII – os recursos provenientes de acordos, convênios ou contratos celebrados com entidades, organismos ou empresas, públicos ou privados, nacionais ou internacionais;

VIII – o produto da venda de publicações, material técnico, dados e informações, inclusive para fins de licitação pública.

Seção II

Do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

Art. 58. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto de 23 (vinte e três) representantes titulares, e seus suplentes, dos seguintes órgãos:

- I – 6 (seis) representantes do Poder Executivo federal;
- II – 1 (um) representante indicado pelo Senado Federal;
- III – 1 (um) representante indicado pela Câmara dos Deputados;
- IV – 1 (um) representante indicado pelo Conselho Nacional de Justiça;
- V – 1 (um) representante indicado pelo Conselho Nacional do Ministério Público;
- VI – 1 (um) representante indicado pelo Comitê Gestor da Internet no Brasil;
- VII – 4 (quatro) representantes da sociedade civil com atuação comprovada em proteção de dados pessoais;
- VIII – 4 (quatro) representantes de instituição científica, tecnológica e de inovação; e
- IX – 4 (quatro) representantes de entidade representativa do setor empresarial afeto à área de tratamento de dados pessoais.

§ 1º Os representantes serão designados por ato do Presidente da República, permitida a delegação, e terão mandato de 2 (dois) anos, permitida 1 (uma) recondução.

§ 2º A participação no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será considerada atividade de relevante interesse público e não será remunerada.

§ 3º Os representantes referidos nos incisos I a VI do *caput* deste artigo e seus suplentes serão indicados pelos titulares dos respectivos órgãos e entidades.

§ 4º Os representantes referidos nos incisos VII, VIII e IX do *caput* deste artigo e seus suplentes serão indicados na forma de regulamento e não poderão ser membros da entidade mencionada no inciso VI do *caput* deste artigo.

Art. 59. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade:

I – propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD;

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 pela ANPD;

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 da privacidade à população.

CAPÍTULO X

DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 60. A Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), passa a vigorar com as seguintes alterações:

“Art. 7º

.....

X – exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais;

.....” (NR)

“Art. 16.

.....

II – de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a proteção de dados pessoais.” (NR)

Art. 61. A empresa estrangeira será notificada e intimada de todos os atos processuais previstos nesta Lei, independentemente de procuraçāo ou de disposição contratual ou estatutária, na pessoa do agente ou representante ou pessoa responsável por sua filial, agência, sucursal, estabelecimento ou escritório instalado no Brasil.

Art. 62. A autoridade nacional e o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep), no âmbito de suas competências, editarão regulamentos específicos para o acesso a dados tratados pela União para o cumprimento do disposto no § 2º do art. 9º da Lei nº 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional), e aos referentes ao Sistema Nacional de Avaliação da Educação Superior (Sinaes), de que trata a Lei nº 10.861, de 14 de abril de 2004.

Art. 63. A autoridade nacional estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados.

Art. 64. Os direitos e princípios expressos nesta Lei não excluem outros relacionados à matéria previstos no ordenamento jurídico pátrio ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Art. 65. Esta Lei entra em vigor após decorridos 18 (dezoito) meses de sua publicação oficial.