

**COMISSÃO ESPECIAL DESTINADA A PROFERIR PARECER AO
PROJETO DE LEI Nº 4060, DE 2012**

(TRATAMENTO E PROTEÇÃO DE DADOS PESSOAIS)

SUBSTITUTIVO AO PROJETO DE LEI Nº 4.060, DE 2012

(Apenso PLs nºs 5.276/16 e 6.291/16)

Estabelece a Lei Geral de Proteção de
Dados.

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 fundamento o respeito à privacidade e:

I – a autodeterminação informativa;

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

4

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

IV – o desenvolvimento econômico, tecnológico e a inovação;

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

VI – os direitos humanos e o livre desenvolvimento da personalidade, dignidade e 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, salvo o tratamento previsto no inciso IV do art. 4º;

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; 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 pessoais:

I – realizado por pessoa natural para fins exclusivamente pessoais;

II – realizado para fins exclusivamente:

a) jornalísticos e artísticos; ou

b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11;

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

IV – provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou 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 previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observado o devido processo legal e 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, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico ao órgão competente e que deverão observar a limitação imposta no § 4º.

§ 3º Órgão competente emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.

§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III poderão ser tratados por pessoa de direito privado.

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

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

II – dados sensíveis: dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou

a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural;

III – dados anonimizados: dados pessoais relativos a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

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

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

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

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

VIII – encarregado: pessoa natural, indicada pelo responsável, que atua como canal de comunicação entre o responsável e os titulares e o órgão competente;

IX – agentes do tratamento: o responsável e o operador;

X – 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;

XI – anonimização: utilização de meios técnicos razoáveis e disponíveis quando do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

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

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

XIV – eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independente do procedimento empregado;

XV – transferência internacional de dados: transferência de dados pessoais para um país estrangeiro ou organização internacional da qual o país seja membro;

XVI – 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 esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidos por esses entes públicos, ou entre entes privados;

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

XVIII – 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;

XIX – órgão competente: órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento desta Lei.

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 propósitos legítimos, específicos, explícitos e informados ao titular, não podendo ser tratados posteriormente de forma incompatível com essas finalidades;

II – adequação: pelo qual o tratamento deve ser compatível com as finalidades informadas ao 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 a forma e a duração do tratamento, bem como sobre a integralidade dos seus dados pessoais;

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

VI – transparência: pelo qual devem ser garantidas aos titulares 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: pelo qual devem ser utilizadas medidas 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 difusão;

VIII – prevenção: pelo qual devem ser adotadas medidas para 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 ilícitos ou abusivos;

X – responsabilização e prestação de contas: pelo qual o agente deve demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, incluindo a eficácia das medidas.

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 de consentimento pelo titular;

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

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

IV – para a realização de estudos por órgão de pesquisa, sendo 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, administrativo ou arbitral, nos termos da Lei nº 9.307, de 23 de setembro de 1996;

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 ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X – para proteção do crédito de acordo com o art. 43 da Lei nº 8.078, de 11 de setembro de 1990, que dispõe sobre a proteção do consumidor.

§ 1º Nos casos de aplicação do disposto nos incisos II e III e excetuadas as hipóteses previstas no art. 4º, 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 art. 23 poderá ser especificada pelo órgão competente.

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

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

§ 5º O responsável que obteve o consentimento a que faz referência o inciso I que necessitar comunicar ou compartilhar dados pessoais com outros responsáveis 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 do tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

Art. 8º O consentimento previsto no art. 7º, inciso I, 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, este deverá ser provido em cláusula destacada de 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 mediante vício de consentimento.

§ 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, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob o amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do art. 18.

§ 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º, o responsável deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

Art. 9º O titular tem o direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma

clara, adequada e ostensiva sobre, 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 responsável;

IV – informações de contato do responsável;

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

VI – responsabilidades dos agentes que realizarão o tratamento;

e

VII – direitos do titular, com menção explícita aos direitos contidos no art. 18.

§ 1º Na hipótese em que o consentimento é requerido, este 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 é requerido, havendo mudanças da finalidade para o tratamento de dados pessoais não compatível com o consentimento original, o responsável deverá informar previamente ao titular sobre as mudanças de finalidade, podendo o titular 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 tal fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18.

Art. 10. O legítimo interesse do responsável somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem:

I – o apoio e a promoção de atividades do responsável; e

II – em relação ao titular, a proteção do exercício regular de seus direitos ou a 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 responsável, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§ 2º O responsável deverá adotar medidas para garantir a transparência do tratamento de dados baseado no seu legítimo interesse.

§ 3º O órgão competente poderá solicitar ao responsável relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento o seu interesse legítimo, observados os segredos comercial e industrial.

Seção II

Dados Sensíveis

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

I – com fornecimento de consentimento específico e em destaque, pelo titular, para finalidades específicas;

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 necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

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

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

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

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

g) garantir a prevenção à fraude e a segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º e exceto no caso no caso de prevalecerem 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 pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do art. 23.

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

Art. 12. Os dados anonimizados serão considerados dados pessoais, para os fins desta Lei, 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 necessário 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 a formação do perfil comportamental de uma determinada pessoa natural, se identificada.

§ 3º O órgão competente poderá dispor sobre padrões e técnicas utilizadas em processos de anonimização, e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.

Art. 13. Na realização de estudos 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 pseudomização 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 pesquisa de que trata o caput em nenhuma hipótese poderá revelar dados pessoais.

§ 2º O órgão de pesquisa será o responsável pela segurança da informação prevista no caput, não sendo permitida, em qualquer circunstância, a transferência dos dados a terceiros.

§ 3º O acesso aos dados de que trata este artigo será objeto de regulamentação por parte do órgão competente e das autoridades da área de saúde e sanitárias, no âmbito de suas respectivas 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 através do uso de informação adicional mantida separadamente pelo responsável em ambiente controlado e seguro.

Seção III

Crianças e Adolescentes

Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado no seu melhor interesse, nos termos deste artigo e da legislação pertinente.

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

§ 2º Os responsáveis pelo tratamento de dados de que trata o § 1º deverão manter pública informação sobre os tipos de dados coletados, como estes são utilizados e os procedimentos para o exercício dos direitos a que se refere o art. 18.

§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º quando a coleta se faça necessária para contatar os pais ou responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção e em nenhum caso poderão ser repassados a terceiros sem o consentimento de que trata o § 1º.

§ 4º Os responsáveis por tratamento de dados não devem condicionar a participação dos titulares de que trata o § 1º a jogos, aplicações

de internet ou outras atividades ao fornecimento de mais informações pessoais que as estritamente necessárias para participar da atividade.

§ 5º O responsável deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º foi dado pelo responsável pela criança, levando em consideração as tecnologias disponíveis.

§ 6º As informações referentes ao tratamento de dados referidas no § 3º deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptiva, sensoriais, intelectuais e mentais do usuário, utilizando recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou responsável legal e também adequadas ao entendimento da criança.

Seção IV

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 ao 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 § 5º do art. 8º, resguardado o interesse público; ou

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

Art. 16. 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 do responsável;

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

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

IV – para uso exclusivo do responsável, sendo vedado o seu acesso por terceiros e desde que anonimizados.

CAPÍTULO III

DOS 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 do responsável em relação aos dados por ele tratados, a qualquer momento e mediante requisição, 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 de seus dados pessoais a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão responsável;

VI – eliminação, de dados pessoais com cujo tratamento o titular tenha consentido, exceto nas hipóteses previstas no art. 16;

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

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

IX – a revogação do consentimento nos termos do § 5º do art. 8º; e

X – peticionar contra responsável perante o órgão competente e os organismos de defesa do consumidor.

§ 1º O titular pode se opor 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 expresso do titular, representantes legalmente constituídos, a um dos agentes de tratamento.

§ 3º Em caso de impossibilidade de adoção imediata da providência de que trata o § 2º, o responsável enviará ao titular resposta em que poderá:

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

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

§ 4º O requerimento de que trata o § 2º será atendido sem custos para o titular nos prazos e termos previstos na regulamentação.

§ 5º O responsável deverá informar de maneira imediata aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, eliminação, anonimização ou bloqueio dos dados, para que repitam idêntico procedimento.

§ 6º A portabilidade dos dados pessoais a que se refere o inciso V do caput não inclui dados que já tenham sido anonimizados pelo responsável.

Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:

I – em formato simplificado, imediatamente; ou

II – por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 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 tal fim; ou

II – sob forma impressa.

§ 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral dos seus dados pessoais, observado o segredo comercial e industrial, nos termos da regulamentação do órgão competente, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

§ 4º O órgão competente poderá dispor de forma diferenciada acerca dos prazos dos incisos I e II do caput para os setores específicos.

Art. 20. 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 as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo, de crédito ou aspectos de sua personalidade.

§ 1º O responsável 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 oferecimento de informações de que trata o § 1º baseado na observância de segredo comercial e industrial, o órgão competente poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizados de dados pessoais.

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

Art. 22. A defesa dos interesses e dos 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 art. 81 e art. 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 IV

DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

Seção I

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, desde que:

I – sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, finalidade, procedimentos e 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, no âmbito da Lei que menciona o caput, sendo vedado seu compartilhamento no âmbito do Poder Público e com pessoas jurídicas de direito privado; e

III – seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei.

§ 1º O órgão competente poderá dispor sobre as formas pelas quais se dará a publicidade das operações de tratamento.

§ 2º O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no caput de instituir as autoridades de que trata a Lei que menciona o caput.

§ 3º 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, da Lei nº 9.784, de 29 de janeiro de 1999 e da Lei nº 12.527, de 18 de novembro de 2011.

§ 4º Os serviços notariais de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas de que trata o caput nos termos desta Lei.

§ 5º Os serviços notariais de registro devem fornecer acesso aos dados por meio eletrônico para a Administração Pública, tendo em vista as finalidades de que trata o caput.

Art. 24. As empresas públicas e as 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 as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução desta, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos deste Capítulo.

Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado para a execução de políticas públicas, prestação de serviços públicos, a descentralização da atividade pública e a disseminação e o 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 elencados 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 o exija e exclusivamente para este fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011;

II – quando houver previsão legal e a transferência seja 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 e convênios de que trata o § 1º deverão ser comunicados ao órgão competente.

Art. 27. A comunicação ou o uso compartilhado 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, exceto:

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

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

III – nas exceções constantes no § 1º do art. 26.

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

Art. 29. O órgão competente poderá solicitar, a qualquer momento, às entidades do Poder Público a realização de 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 ou o uso compartilhado 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.

Art. 32. O órgão competente poderá solicitar a agentes do poder público a publicação de relatórios de impacto à proteção de dados pessoais e poderá sugerir a adoção de padrões e boas práticas aos tratamentos de dados pessoais pelo poder público.

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 organizações internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;

II – quando o responsável 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 uma determinada transferência;

4

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

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

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

V – quando o órgão competente autorizar a transferência;

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

VII – quando a transferência for necessária para execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do art. 23 desta Lei;

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

IX – quando necessário para atender as hipóteses previstas no art. 7º, inciso II, V e VI.

Parágrafo único. Para os fins do inciso I do art. 33 desta Lei, pessoas jurídicas de direito público referenciadas no parágrafo único do art. 1º da Lei 12.527, de 18 de novembro de 2011, no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer ao órgão competente a avaliação do nível de proteção a dados pessoais conferido por país ou organização internacional.

Art. 34. O nível de proteção de dados do país estrangeiro ou da organização internacional mencionado no inciso I do art. 33, será avaliado pelo órgão competente, que levará em conta:

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

II – a natureza dos dados;

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

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

V – as outras circunstâncias específicas relativas à transferência; e

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

Art. 35. A definição do conteúdo de cláusulas contratuais padrão, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, a que se refere o inciso II do art. 33, será realizado pelo órgão competente.

§ 1º Para a verificação do previsto no caput deste artigo deverão ser considerados os requisitos, condições e garantias mínimas para a transferência que observe os direitos, garantias e princípios desta lei;

§ 2º Na análise de cláusulas contratuais, de 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, quando necessário.

§ 3º O órgão competente poderá designar organismos de certificação para a realização do previsto no caput deste artigo, que permanecerão sob sua fiscalização nos termos definidos em regulamento.

§ 4º Os atos realizados por organismo de certificação poderão ser revistos pelo órgão competente e, caso em desconformidade com esta Lei, submetidos à revisão ou anulados.

§ 5º 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 § 1º e § 2º do art. 46.

Art. 36. Alterações nas garantias apresentadas como suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no inciso II do art. 33 deverão ser comunicadas ao órgão competente.

CAPÍTULO VI

DOS AGENTES DO TRATAMENTO DE DADOS PESSOAIS

Seção I

Responsável e operador

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

Art. 38. O órgão competente poderá determinar ao responsável que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente às suas operações de tratamento de dados, nos termos do regulamento, observados os segredos comercial e industrial.

Parágrafo único. Observado o disposto no caput, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a

metodologia utilizada para sua coleta e para a garantia da segurança das informações, bem como a análise do responsável com relação às medidas, salvaguardas e mecanismos de mitigação de risco adotados.

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

Art. 40. O órgão competente poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso dos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.

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 no sítio eletrônico do responsável.

§ 2º As atividades do encarregado consistem em:

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

II – receber comunicações do órgão competente e adotar providências;

III – orientar os funcionários e os 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 o porte da entidade ou o volume de operações de tratamento de dados.

Seção III

Responsabilidade e ressarcimento de danos

Art. 42. O responsável 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 responsável, hipótese em que o operador equipara-se a responsável, salvo as hipóteses de exclusão do art. 43.

II – responsáveis que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo as hipóteses de exclusão do art. 43.

§ 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 quando 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, podem ser exercidas a título coletivo em juízo, nos termos do Título III, da Lei 8.078, de 11 de setembro de 1990, que dispõe sobre a proteção do consumidor.

§ 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;

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 dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais:

I – o modo pelo qual é realizado;

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

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

Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o responsável ou o operador, que ao deixar de adotar as medidas de segurança previstas no art. 43, der causa ao dano.

Art. 45. As hipóteses de violação ao direito do titular no âmbito das relações de consumo permanecem inteiramente sujeitas às regras de responsabilidade previstas na Lei 8.078, de 11 de setembro de 1990, observado o inciso III do art. 4º daquela lei.

CAPÍTULO VII

DA SEGURANÇA E DAS BOAS PRÁTICAS

Seção I

Segurança e 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 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 mínimos 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, assim como os princípios previstos no art. 6º desta Lei.

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

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

Art. 48. O responsável deverá comunicar ao órgão competente 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 pelo órgão competente, e deverá mencionar, no mínimo:

- I – a descrição da natureza dos dados pessoais afetados;
- II – as informações sobre os titulares envolvidos;
- III – a indicação das 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 da comunicação não ter sido imediata; e
- VI – as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos de prejuízo.

§ 2º 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 providências, 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 terceiros não autorizados 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, padrões de boas práticas e de governança, aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Seção II

Boas práticas e Governança

Art. 50. Os responsáveis e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos 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, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios, decorrentes de tratamento de dados de titular.

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

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

a) demonstre o comprometimento do responsável 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 em que se deu sua coleta;

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

d) estabeleça políticas e salvaguardas adequadas a partir de 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 e que assegure mecanismos de participação do titular;

f) esteja integrado à 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 do órgão competente ou de outra entidade responsável por promover o cumprimento 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 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

DA FISCALIZAÇÃO

Seção I

Sanções administrativas

Art. 52. As infrações realizadas por agentes de tratamento de dados às normas previstas nesta Lei ficam sujeitas às seguintes sanções administrativas aplicáveis pelo órgão competente:

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

II – multa simples ou diária, de até 2% 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 – publicização da infração após devidamente apurada e confirmada a sua ocorrência;

IV – bloqueio de dados pessoais a que se refere a infração, até a sua regularização;

V – eliminação de dados pessoais a que se refere a infração; e

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

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

VIII – 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 cumulativamente, de acordo com as peculiaridades do caso concreto 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 – ao grau 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; e

XI – a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

§ 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 e de III a VIII do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do

disposto nas Leis nºs 8.112, de 11 de dezembro de 1990, 8.429, de 2 de junho de 1992 e 12.527, de 18 de novembro de 2011.

§ 4º No cálculo do valor da multa de que trata o inciso II do caput deste artigo, o órgão competente 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 pelo órgão competente, ou quando este for apresentado de forma incompleta e/ou não demonstrado de forma inequívoca e idônea.

Art. 53. O órgão competente definirá, por meio de regulamento próprio de 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 devem ser previamente publicadas, para ciência dos agentes de tratamento, e 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 devem estabelecer as circunstâncias e condições para a adoção de multa simples ou diária.

Art. 54. O valor da sanção de multa diária, que vem a ser aplicável às infrações a esta Lei, deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pelo órgão competente.

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

Seção II

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

Art. 54. Fica criado o órgão competente, Autoridade Nacional de Proteção de Dados, entidade integrante da Administração Pública Federal indireta, submetida a regime autárquico especial e vinculada ao Ministério da Justiça.

§ 1º A Autoridade deverá ser regida nos termos previstos na Lei nº 9.986, de 18 de julho de 2000.

§ 2º A Autoridade terá como órgão máximo o Conselho Diretor, devendo contar também com um Conselho Nacional de Proteção de Dados e da Privacidade, além das unidades especializadas para a aplicação desta Lei.

§ 3º A natureza de autarquia especial conferida à Autoridade 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 Autoridade serão aprovados por decreto do Presidente da República.

§ 5º O Conselho Diretor será composto por três conselheiros e decidirá por maioria.

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

§ 7º Os mandatos dos primeiros membros do Conselho Diretor serão de três, quatro, cinco anos, a serem estabelecidos no decreto de nomeação.

4 § 8º É vedado ao ex-conselheiro utilizar informações privilegiadas obtidas em decorrência do cargo exercido, sob pena de incorrer em improbidade administrativa.

Art. 55. O órgão competente terá as seguintes atribuições:

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

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

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

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

V – atender petições de titular contra responsável;

VI – promover entre a população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e as medidas de segurança;

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, que deverão levar em consideração 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 transacional;

X – dispor sobre as formas pelas quais se dará a publicidade das operações de tratamento, observando o respeito ao segredo comercial e industrial;

4

XI – 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;

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; e

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, devendo publicar no relatório de gestão a que se refere o inciso XII o detalhamento de suas receitas e despesas;

XVI – realizar ou determinar a realização de auditorias, no âmbito da atividade de fiscalização, sobre o tratamento de dados pessoais realizado 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, o órgão competente deve observar a exigência de mínima intervenção, assegurando fundamentos, princípios e direitos dos titulares previstos no art. 170 da Constituição Federal e nesta Lei.

§ 2º Os regulamentos e normas editados pelo órgão competente devem necessariamente precedidos de consulta e audiência públicas, bem como de análises de impacto regulatório.

Art. 56. Constituem receitas do órgão competente:

- I – o produto da execução da sua dívida ativa;
- II – as dotações consignadas no Orçamento-Geral da União, créditos especiais, créditos adicionais, transferências e repasses que lhe forem conferidos;
- III – as doações, legados, subvenções e outros recursos que lhe forem destinados;
- IV – os valores apurados na venda ou aluguel de bens móveis e imóveis de sua propriedade;
- V – os valores apurados em aplicações no mercado financeiro das receitas previstas neste artigo;
- VI – produto da cobrança de emolumentos por serviços prestados;
- VII – recursos provenientes de acordos, convênios ou contratos celebrados com entidades, organismos ou empresas, públicos ou privados, nacionais e internacionais;
- VIII – produto da venda de publicações, material técnico, dados e informações, inclusive para fins de licitação pública.

Art. 57. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto por vinte e três representantes titulares, e seus respectivos suplentes, dos seguintes órgãos:

- I – seis representantes do Poder Executivo Federal;
- 4 II – um representante indicado pelo Senado Federal;
- III – um representante indicado pela Câmara dos Deputados;

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 – quatro representantes da sociedade civil com atuação comprovada em proteção de dados pessoais;

VIII – quatro representantes de instituição científica, tecnológica e de inovação ; e

IX – quatro representantes de entidade representativa do setor empresarial afeito 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 dois anos, permitida uma recondução.

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

§ 3º Os representantes referidos no inciso I a VI do caput e seus respectivos suplentes serão indicados pelos titulares dos respectivos órgãos e entidades.

§ 4º Os representantes referidos nos incisos VII a IX do caput e seus respectivos suplentes serão indicados na forma do regulamento e não poderão ser membros da entidade mencionada no inciso VI.

Art. 58. 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 de atuação do órgão competente;

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 FINAIS E TRANSITÓRIAS

Art. 59. Esta Lei entra em vigor 18 (dezoito) meses após a data de sua publicação.

Parágrafo único. O órgão competente estabelecerá normas sobre a 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.

Art. 60. A empresa estrangeira será notificada e intimada de todos os atos processuais previstos nesta Lei, independentemente de procuração 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. 61. O órgão competente e o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP), no âmbito de suas respectivas

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 dezembro de 1996, que estabelece as diretrizes e base da educação nacional, e os 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. 62. O inciso X, do art. 7º, e o inciso II, do art. 16, da Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, passarão a vigorar com a seguinte redação:

“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 trata da 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 trata da proteção de dados pessoais.” (NR)

Art. 63. Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Sala da Comissão, em de de 2018.


Deputado Orlando Silva
Relator