

PARECER Nº , DE 2018

Da COMISSÃO DE ASSUNTOS ECONÔMICOS, sobre o Projeto de Lei do Senado nº 330, de 2013, do Senador Antonio Carlos Valadares, que *dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências*, sobre o Projeto de Lei do Senado nº 131, de 2014, de autoria da Comissão Parlamentar de Inquérito da Espionagem (CPIDAESP), que *dispõe sobre o fornecimento de dados de cidadãos ou empresas brasileiros a organismos estrangeiros*, e sobre o Projeto de Lei do Senado nº 181, de 2014, do Senador Vital do Rêgo, que *estabelece princípios, garantias, direitos e obrigações referentes à proteção de dados pessoais*.

Relator: Senador **RICARDO FERRAÇO**

I – RELATÓRIO

Veem ao exame desta Comissão os Projetos de Lei do Senado (PLS) **nº 330, de 2013**, do Senador Antonio Carlos Valadares; **nº 131, de 2014**, de autoria da Comissão Parlamentar de Inquérito da Espionagem (CPIDAESP); **e nº 181, de 2014**, do Senador Vital do Rêgo, os quais tramitam em conjunto após a aprovação dos Requerimentos nº 992 a 998, ambos de 2014.

Perante a CCT e a CMA, as matérias foram relatadas pelo então Senador Aloysio Nunes Ferreira. Seu relatório legislativo, perante a CCT, concluiu pela apresentação de uma Emenda Substitutiva, adotada em parecer



SF/18051.14988-53

unânime daquela Comissão, inclusive incorporando emendas apresentadas por outros parlamentares, e chancelada pela Comissão subsequente, CMA.

Em 03/10/2017, apresentei relatório favorável a este Projeto de Lei, nos termos do substitutivo aprovado na Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática, e pela Comissão de Meio Ambiente. Opinei, ainda, pela rejeição da Emenda nº 32 e das Subemendas à Emenda nº 31-CCT-CMA apresentadas até então, além da declaração de prejudicialidade dos projetos apensados. Concluí, por fim, meu relatório com a apresentação de 24 subemendas de relator.

Além da realização de duas audiências públicas em Comissões, o assunto foi, também, por iniciativa desta Relatoria, discutido em Sessão de Debates Temáticos, no Plenário desta Casa, ocorrida no dia 17/04/2018, com a presença de especialistas, representantes da sociedade civil e do governo federal.

As contribuições foram notadamente relevantes, ao ponto de terem sido consideradas no presente Relatório.

Ao total, foram ainda apresentadas, perante esta Comissão, 1 emenda, recebida como número 32, e outras 14 subemendas à Emenda Substitutiva nº 31 – CCT/CMA, de autoria de diversos Senhores Senadores.

Nada mais há que se relatar.

II – ANÁLISE

II.1 Aspectos formais:

Nos termos do art. 99, do Regimento Interno do Senado Federal (RISF), compete à Comissão de Assuntos Econômicos (CAE) opinar sobre “aspecto econômico e financeiro de qualquer matéria que lhe seja submetida” (inc. I) e também sobre “proposições pertinentes aos problemas econômicos do país” (inc. III).

No que diz respeito aos aspectos formais das propostas, não vislumbramos vício de qualquer natureza. A matéria é constitucional, preenche



os requisitos de juridicidade e regimentalidade e encontra-se em plena conformidade com a melhor técnica legislativa.

Ademais, a proposta tem o atributo da generalidade, possui potencial de coercitividade e inova o ordenamento jurídico.

II.1 Mérito:

No mérito, já pudemos discorrer acerca da oportunidade e da urgência de aprovação do presente marco legal de proteção de dados. Não se trata de uma opção legislativa, mas uma necessidade inafastável. Reconhecemos, pois, a importância ímpar do projeto.

A despeito do contexto de crise econômica, é seguro afirmar que o País tem perdido oportunidades valiosas de investimento financeiro internacional em razão do isolamento jurídico em que se encontra por não dispor de uma lei geral e única de proteção de dados pessoais (LGPD).

O dado pessoal é hoje insumo principal da atividade econômica em todos os setores possíveis. É, ainda, como já afirmamos, elemento fundamental até mesmo para a concretização de políticas públicas, dado o elevado grau de informatização e sistematização do Estado brasileiro, em todos os níveis federativos. Mais que isso: o dado pessoal é um ingrediente importante da privacidade da pessoa humana e sua preservação (ou violação) guarda relação direta com a maneira com que empresas ou governos se utilizam dos dados do cidadão.

Por isso, regras claras são fundamentais para assegurar a conformidade da atividade econômica em um cenário de máxima confiabilidade do cidadão, quanto ao respeito a direitos fundamentais que lhes são caros.

A bem da verdade, a sociedade brasileira, pouco habituada à cultura de valorização de dados pessoais, pouco a pouco se conscientiza sobre a importância da privacidade para uma experiência de vida digna, vindo a reclamar, cada vez mais, a aprovação de um marco regulatório que estabeleça diretrizes mínimas de proteção de dados.



Alinhamo-nos, assim, ao resto do mundo: já se tem notícia de 125 países com leis de proteção de dados, sendo o Brasil um dos poucos ainda a não deliberar sobre a questão, o que é inadmissível.

Deparamo-nos, na verdade, com uma lacuna que muito impacta e obstrui o pleno desenvolvimento econômico e o progresso brasileiro

Na proposta de normatização da sociedade brasileira na era digital, o Governo brasileiro previu a efetivação de três vertentes regulatórias baseadas na informação: a regulamentação do acesso à informação pública (efetivada através da edição da Lei nº 12.527/2011 – Lei de Acesso à Informação), a regulação do uso da internet no Brasil (efetivada através da aprovação do Marco Civil da Internet) e a proposta de edição de um marco regulatório de proteção de dados pessoais, que ora promovemos.

Estamos seguros de que, finda esta nobre missão, e uma vez sancionada a Lei Geral de Proteção de Dados Pessoais - LGPD, o País entrará definitivamente na rota dos principais investimentos comerciais e econômicos internacionais, bem como no seleto grupo de Países que demonstram respeito e conferem efetividade e importância à proteção da privacidade de seus cidadãos.

Note-se que a inércia brasileira na aprovação desta lei geral tem sido de tal forma insuportável, que órgãos do Ministério Público já estão se mobilizando, amparados em uma frágil e setORIZADA regulação da questão no Brasil.

Foi o caso da criação da Comissão de Proteção dos Dados Pessoais no âmbito do Ministério Público do Distrito Federal e Territórios (MPDFT). Com atuação dedicada a opinar, informar, cooperar, promover estudos, notificar, investigar e sancionar, a iniciativa tem focado nos recentes episódios de vazamento ou utilização ilegítima de dados pessoais por empresas que realizam esse tipo de tratamento.

Referida iniciativa, já em intensa atuação, na verdade, transmite uma mensagem forte ao Congresso Nacional: a premência urgente de aprovação desta lei e, mais ainda, de definição acerca da criação de uma autoridade central de proteção de dados pessoais.



Um dos casos sob investigação do MPDFT, por exemplo, foi o recente episódio envolvendo o acesso indevido e o uso ilegítimo de dados pessoais de centenas de milhares de brasileiros coletados a partir de uma rede social norteamericana por uma empresa de consultoria estratégica em mídias sociais do Reino Unido, que utilizava recursos avançados de mineração e análise estratégica de dados.

O caso reverberou no mundo todo e trouxe à tona a necessidade de regulações com maior grau de proteção sobre o tratamento de dados pessoais de cidadãos, sobretudo pela sensibilidade da questão: manipulação eleitoral e política.

Enfim, com o objetivo de simplificar nosso trabalho, socorremo-nos, aqui, da narrativa, dos argumentos e das opiniões já lançadas em nosso relatório anterior, a qual reiteramos, para, nesta fase do processo legislativo, registrar opinativo focado nas emendas apresentadas e nas sugestões colhidas no debate público com a sociedade e o governo federal. Aliás, convém destacar que, no período de reexame deste relatório, esta relatoria colheu sugestões encaminhadas a meu gabinete pelo Governo Federal, através de órgãos vinculados à Casa Civil.

Sem prejuízo de novas impressões que vierem a serem colhidas, limitamo-nos a extrair, dessas contribuições, um texto que efetivamente reverbere opiniões consensuais, limitando os pontos de maior distensão para que sejam amadurecidos em debate público e transparente. Aproveitou-se, assim, o que havia de mais moderno e adequado, dentre as sugestões plurais que recebemos.

Assim sendo, tendo em vista as referidas colaborações, em especial as emendas apresentadas, que muito enriquecem o processo legislativo plural e democrático, o relatório sofreu alterações.

Oportunamente, foram apresentadas 15 emendas ou subemendas perante esta Comissão.



II.1.1 Emendas apresentadas

A eminente Senadora Marta Suplicy apresentou a **Emenda nº 32** e as **Subemendas nºs 1 e 2**, à Emenda nº 31-CCT-CMA, que, em apertada síntese:

1. Excepciona, da incidência normativa da lei, os bancos de dados das serventias notariais e de registro; e
2. Delineia regras específicas de tratamento de dados pessoais quando voltadas a registros em cadastros de crédito negativadores;
3. Prevê regras específicas para inclusão de dados restritivos ao crédito em decorrência de dívida.

No entanto, a despeito do mérito das sugestões trazidas pela nobre Senadora Marta Suplicy, não podemos com elas concordar. Isso porque a proposta aqui formulada é de definição de uma lei geral de proteção de dados pessoais, sem descer ao detalhamento das relações jurídicas possíveis nos infindáveis setores de atuação pública ou privada, por meio dos quais essas informações trafegarão.

De se notar, ainda, que estamos alinhados às principais normas internacionais, que estabelecem pontuais e mínimas exceções à aplicabilidade desse regramento especial, aliás, em consonância com as Diretrizes da própria Organização para a Cooperação e Desenvolvimento Económico ou Económico (OCDE), cujo ingresso o Brasil pleiteia atualmente.

Por tal razão, a fim de incorrer em uma norma sem observância da devida isonomia de tratamento normativo e, ainda, sem incorrer em vícios de juridicidade, em razão das regras cogentes de elaboração de leis previstas na Lei Complementar nº 95, de 1998, opinamos por sua **rejeição**.

O nobre Senador José Medeiros apresentou as seguintes Subemendas:



1. **Subemenda nº 3:** objetiva tornar claro que o consentimento, na condição de direito do titular, compreende ainda o tratamento dos dados pessoais mediante o uso de Internet;
2. **Subemenda nº 4:** a proposta amplia as hipóteses de transferência internacional de dados para Países que não proporcionam nível homogêneo ao brasileiro na proteção de dado, para prever, ainda, que esse fluxo de comunicação seja possível quando o responsável pelo tratamento dos dados oferecer e comprovar garantias de cumprimento das regras e garantias protetivas da lei, na forma de “cláusulas contratuais padrão” e “de selos, certificados e códigos de conduta e adequação emitidos por organismos de certificação qualificados”, através ora da autoridade competente, ora de organismos de certificação qualificados;
3. **Subemenda nº 5:** simplifica as regras de aplicabilidade da LGPD, no que diz respeito ao tratamento de dados de crianças e adolescentes, remetendo a questão a normas especiais, como o Estatuto da Criança e do Adolescente, além do Código Civil Brasileiro.

Alinhamo-nos às três propostas apresentadas, na forma do Substitutivo ao final apresentado.

De fato, é evidente que a LGPD deve se aplicar inclusive ao tratamento de dados pessoais havido através da internet. Nesse aspecto, inclusive, propomos a derrogação do microrregime de proteção de dados presente na Lei nº 12.965, de 2014, a fim de evitar incongruências e incompatibilidade, além de estabelecer maior segurança jurídica. Dessa forma, entendemos contemplada a **Subemenda nº 3**.

A **Subemenda nº 4**, igualmente acolhida, trata, como bem lembra o autor da proposta, de incorporar instrumentos modernos de regulação do fluxo internacional de dados, presentes tanto no sistema *Cross-Border Privacy Rules* (CBPR, em inglês), desenvolvido e adotado no âmbito do Foro de Cooperação Econômica Ásia-Pacífico (APEC, em inglês), como no âmbito da Regulação Geral de Proteção de Dados - RGPD (GPDR, em inglês), norma europeia que muito tem influenciado nossos trabalhos.

O propósito, também parafraseando o autor, é “assegurar mecanismos de transferência de dados que permitam transferências não apenas dentro de um mesmo grupo corporativo global, mas também entre empresas não afiliadas”. Somos, assim, por sua aprovação.

De outro lado, a **Subemenda nº 5** está totalmente acatada, na medida em que uma análise mais detida aproximou este texto daquele inspirado no PL 5276, de 2016, de iniciativa do Poder Executivo, que tramita na Câmara dos Deputados.

A **Subemenda nº 6**, de iniciativa do Senador Valdir Raupp, objetiva expandir o conceito de dados pessoais sensíveis, para estabelecer dados biométricos na categoria de dados sensíveis, bem como vincular tais dados expressamente ao histórico médico do titular dos dados. Seu objetivo é precisão da redação, ao mesmo tempo em que se estabelece uma definição mais abrangente.

Entendemos que o Substitutivo ora proposto contempla esta sugestão, na medida em que redefine dado pessoal sensível como sendo “qualquer dado pessoal que revele a orientação religiosa, política ou sexual, a convicção filosófica, a procedência nacional, a origem racial ou étnica, a participação em movimentos políticos ou sociais, informações de saúde, genéticas ou biométricas do titular dos dados”.

No entanto, uma melhor técnica legislativa não recomenda, nas normas definidoras de conceitos, destacar uma categorização específica ou a exemplificação isolada das demais. Portanto, somos pelo acatamento parcial da Subemenda, na forma do Substitutivo ora proposto.

A nobre Senadora Vanessa Grazziotin apresentou as **Subemendas nºs 7 a 13**.

A **Subemenda nº 7** delimita em 15 dias corridos o prazo para o responsável pelo tratamento dos dados corrigir e comunicar a retificação dos dados, não merece acolhida. Sustentamos, em nosso parecer, a necessidade de considerar a complexidade de cumprimento dessa norma, que irá inaugurar um novo regime jurídico no Brasil, o que reclama prazo mais compatível com essa realidade. Somos, assim, por sua rejeição.



Entendemos, porém, acolhida a **Subemenda nº 8**, que estabelece prazo de 15 dias úteis para providências imediatas requeridas pelo titular dos dados em caso de imprecisão das informações. Nosso Substitutivo opta por homogeneizar os prazos em 30 dias corridos, de maneira que se encontra parcialmente contemplada referida Subemenda.

A **Subemenda nº 9** trata da definição do regime de solidariedade em caso de dano decorrente da comunicação ou difusão dos dados. Somos por sua aprovação.

A **Subemenda nº 10** versa sobre maior escopo de proteção dos dados pessoais sensíveis. Optamos por remeter a questão à regulamentação da autoridade de proteção, na medida em que ela terá melhores e mais adequadas condições para discorrer sobre os mecanismos de proteção compatíveis com o grau de segurança jurídica que esse tema reclama. Matemos, porém, apenas a necessidade de consentimento diferenciado, mais protetivo, uma vez que tal providência deve ser disposta em lei.

A seu turno, a **Subemenda nº 11** discorre sobre um regime amplo de regulação sobre o dado anonimizado. Entendemos contemplada a proposta, na medida em que nosso Substitutivo, partindo de uma compreensão mais exata do que são (ou deveriam ser) dados anonimizados e como os dados precariamente anonimizados deveriam ser mais bem protegidos. Estes, inclusive, entendemos aproximarem-se, conceitualmente, à proposta inspirada da RGPD e, quanto aos dados pseudonimizados, sobre os quais iremos discorrer mais à frente.

A **Subemenda nº 12** objetiva ampliar o conceito de dados pessoais sensíveis, para contemplar a condição socioeconômica. Discordamos dessa proposta, na medida em que a própria definição jurídica, ou mesmo vernacular, do elemento adjetivador “socioeconômico” é demasiadamente imprecisa e subjetiva, o que daria margem à insegurança jurídica.

A **Subemenda nº 13** importa, da RGPD, o mecanismo de definição legal da qualificadora “identificável”, associada à pessoa natural titular dos dados, na proposta de alargamento do escopo protetivo da lei. Somos por sua rejeição: olvidamos esforços, tanto quanto possível, nesta proposição, para simplificar e objetivar a redação jurídico-legislativa, a fim de evitar

incongruências, confusões, imprecisões. Dessa maneira, o conceito por nós apresentado revela-se já suficiente à aplicação da norma.

Por fim, a **Subemenda nº 14**, de iniciativa do nobre Senador Fernando Bezerra Coelho, busca ampliar as hipóteses de transferência internacional de dados para contemplar o consentimento do titular, uma vez informado do caráter transnacional do fluxo, e, ainda, para permitir que o responsável pelo tratamento, tendo ou não empresa constituída ou estabelecida no Brasil, garanta ao titular o mesmo grau de proteção. Entendemos contemplada a proposta, na forma do Substitutivo ora apresentado.

II.1.2 Emendas de relator

Finda a análise das emendas e subemendas apresentadas, destacamos que reelaboramos nosso relatório para formular, ao final, a propositura de uma nova emenda substitutiva, mais alinhada aos ditames regimentais desta Comissão.

Nosso objetivo foi, de um lado, promover maior alinhamento da proposta presente ao texto do Poder Executivo que se encontra na Câmara dos Deputados, a saber, o PL 5276, de 2016.

Também nos inspiramos fortemente em linhas específicas da norma europeia, por reconhecemos sua relevância para o mundo. A RGPD entrará em vigor no dia 25 de maio do corrente ano e tem provocado mudanças substanciais em todo o globo, em razão de sua característica de extraterritorialidade.

A esse respeito, inclusive, transcrevemos trecho da Nota Técnica que nos foi direcionada, de autoria do Ministério Público Federal:

“(…) não se deve menoscar que para um país em desenvolvimento adotar nas suas linhas gerais um modelo bem sucedido de uma nação desenvolvida ***significa buscar replicar uma experiência institucional que é desejada para a sua sociedade.*** Além do menor custo de não criar uma nova estrutura a partir do nada, se espelhar em profícuas legislações alheias permite acreditar no que se implementou independentemente de eventuais desconfortos iniciais, e garante interlocutores externos que possam



dialogar sobre possíveis ajustes necessários a cada realidade.” (Nota Técnica SCI/PGR 06/2016)

Estamos convictos dessa utilidade cooperativa internacional, quanto ao intercâmbio de experiências e conhecimento.

Respeitamos, porém, as características do Estado e da sociedade brasileiros, que devem, a seu modo, reclamar uma norma própria, nem tanto dissociada dos padrões internacionais já exaustivamente testados pela comunidade global, nem tanto heterogênea ou singular, ao ponto de reclamar um isolamento absoluto do Brasil no cenário internacionais de proteção à privacidade.

Dito isso, destacamos as principais inovações desta relatoria.

Em primeiro lugar, realizamos alterações redacionais, ora relacionadas à uma ainda mais precisa técnica legislativa, ora compatíveis com a estrutura jurídica da própria legislação. Dessa maneira, eliminamos redundâncias conceituais, quando se dispunha, por exemplo, de regras de “tratamento e uso”. Ora, o uso, a coleta, o armazenamento etc. são espécies do gênero “tratamento”. Daí ser impreciso redigir a norma contemplando as duas atividades.

Também evidenciamos que a lei deve se referir à proteção da pessoa natural com relação ao tratamento de seus dados, e não à proteção dos dados pessoais. Uma modificação que sinaliza o devido valor que pretendemos atribuir à norma.

Nessa nova proposta, optamos por conferir uma definição mais adequada aos dados anonimizados, como sendo aqueles que, irreversivelmente, impedem a identificação do titular. Ora, se assim o é, não há sentido em tratar da desanonimização dos dados, eis que o processo anterior deve ser definitivo.

Se os dados, por qualquer razão, podem ser revertidos e reidentificados, então estamos a tratar de dados pseudonimizados¹, um conceito moderno apresentado pela RGD, que inspira maior segurança no tratamento.

¹ Neologismo formado a partir do prefixo *pseudo-*, [falso], com o radical *onom-*, [nome]; mais o sufixo *-izar*, [tornar, transformar].



Além disso, o dado pseudonimizado reclama incentivos, dado seu grau maior de proteção, o que propomos ao longo do texto.

Buscamos, ainda, evidenciar a garantia da liberdade de expressão, comunicação, informação e manifestação do pensamento como princípio, para além de já estarem contemplados nos fundamentos da norma.

Um ponto fulcral, que buscamos afastar, é a noção de que o consentimento deva ser elevado ao status de direito ou princípio. Na verdade, o consentimento é uma das bases legais possíveis para o tratamento dos dados, daí a não ser compatível destaca-lo dos demais, em norma principiológica ou alçado ao nível de direito, posto que as demais hipóteses também são legítimas.

Quanto ao direito ao conhecimento dos critérios e processo de tratamento automatizado dos dados, optamos por aproximar o texto da redação contida, a esse respeito, na Lei do Cadastro Positivo (Lei nº 12.414, de 9 de junho de 2011). Trata-se de importante precedente normativo, já testado socialmente, e que pode ser aqui reproduzido. Note-se que o importante, nesse ponto, não é conferir o direito ao titular de conhecer a finalidade do tratamento, mas, sim, os elementos e critérios que embasam o tratamento de seus dados, com a devida proteção ao segredo empresarial.

Outro ponto de maior equilíbrio entre os interesses do titular e das empresas responsáveis pelo tratamento foi a proposta, inspirada na normativa europeia, de apresentar um mecanismo de contenção de abusos nos requerimentos formulados ao responsável.

Tópico crucial foi a devida normatização do tratamento de dados do setor público. Temos aqui o dever de evidenciar que o poder público deve estar contemplado nesta lei, sendo, possivelmente, o seu principal destinatário. Porém, respeitadas as suas peculiaridades – traduzidas aqui pela finalidade pública e social de suas atribuições, o cumprimento de preceitos constitucionais e legais e a satisfação de políticas públicas que lhe cabem promover.

O devido dimensionamento da atuação do poder público, no âmbito desta lei, confere paridade normativa para o Brasil ser contemplado pela adequação de suas regras de privacidade perante outros países e organismos internacionais.



Nesse espectro, portanto, incorporamos praticamente todas as normas traduzidas ao poder público pelo PL 5.276, de 2016, inclusive quanto ao diálogo deste marco geral com a Lei de Acesso à Informação.

Mais ainda: inspirados em regimes regulatórios vigentes, trouxemos propostas mais adequadas ao uso do poder de polícia pela Administração Pública, com respeito ostensivo ao contraditório e à ampla defesa, e uma atuação jurídica, legal e proporcional, sobretudo baseada no diálogo, e não somente na punição.

O legítimo interesse, por sua vez, foi bem compreendido como instrumento lícito e importante à inovação. Estabelecemos parâmetros mínimos para sua realização, como base legal de tratamento de dados.

Ao final, quanto às sanções administrativas de suspensão e proibição parcial ou total de atividades, ouvimos pleito justo e razoável do setor empresarial e esclarecemos tratarem de punições incidentes sobre atividades específicas, suficientes a fazer cessar a violação de direitos e a penalizar, de forma razoável e proporcional, as empresas.

Inclusive, a esse respeito, fixamos teto para a penalidade de multa, inspirado em parâmetro internacional. Porém, reduzimos a carga dessa sanção específica, a fim de evitar abusos fiscalizatórios. Isso porque a autoridade competente já disporá de diversos outros instrumentos penalizadores, tal como prevemos.

Novamente, nosso objetivo é conferir um maior equilíbrio entre os interesses empresariais e do cidadão, de forma a não desnivelar demasiadamente o eixo de proteção desta norma geral.

Entre as regras transitórias, um ponto merece destaque sobre os demais: considerando os desafios de ordem constitucional, quanto à criação da autoridade central, sugerimos uma saída alternativa, de caráter técnico, a fim de evitar que o Poder Executivo fragmente as atribuições legais ora definidas em mais de um órgão em sua estrutura administrativa e, ao mesmo tempo, respeite a necessidade de atuação técnica para assegurar a aplicabilidade da norma.

Porém, reiteramos, o ideal, a nosso sentir, é a promoção de um órgão próprio, dotado de autonomia e independência técnica, financeira e



institucional, nos moldes do que já tão recomendado pela comunidade internacional.

Sabemos, porém, das dificuldades estruturais das finanças públicas brasileiras no momento atual, razão pela qual adotamos saída intermediária e provisória. Não cessaremos, porém, o diálogo com o Governo Federal, na expectativa de encontrar a melhor solução no médio prazo.

III – VOTO

Ante o exposto, votamos pela **aprovação** do Projeto de Lei do Senado nº 330, de 2013, e, total ou parcialmente, das Subemendas nºs 3, 4, 5, 6, 8, 9, 11, 12 e 14, nos termos da Emenda Substitutiva ora apresentada; pela **rejeição** das demais Emendas e Subemendas; e pela declaração de prejudicialidade do Projeto de Lei do Senado nº 131, de 2014, e do Projeto de Lei do Senado nº 181, de 2014.

EMENDA Nº – CAE (SUBSTITUTIVO)

PROJETO DE LEI DO SENADO Nº 330, DE 2013

Estabelece princípios, garantias, direitos e obrigações referentes à proteção da pessoa natural, quanto ao tratamento de dados pessoais.

O CONGRESSO NACIONAL decreta:

Das Disposições e Princípios Gerais



Art. 1º Esta lei estabelece princípios, garantias, direitos e obrigações referentes à proteção da pessoa natural, quanto ao tratamento de dados de pessoas naturais, tendo como fundamentos:

- I - a autodeterminação informativa;
- II - a liberdade de expressão, de comunicação e de opinião;
- III - a inviolabilidade da intimidade, da vida privada, da honra e da imagem;
- IV - o desenvolvimento econômico e tecnológico; e
- V - a livre iniciativa, a livre concorrência e a defesa do consumidor.

Art. 2º Aplica-se o disposto nesta lei ao tratamento de dados pessoais realizados no todo ou em parte no território nacional ou que nele produza ou possa produzir efeito, qualquer que seja o mecanismo empregado.

§ 1º Esta lei aplica-se:

I - mesmo que a atividade seja realizada por pessoa jurídica sediada no exterior, desde que oferte serviço a indivíduos localizados no território nacional ou pelo menos um integrante do mesmo grupo econômico possua estabelecimento no Brasil;

II - quando a coleta, armazenamento ou utilização dos dados pessoais ocorrer em local onde seja aplicável a lei brasileira por força de tratado ou convenção.

§ 2º 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.

§ 3º Ao tratamento de dados realizado pelo poder público, no atendimento de sua finalidade pública e no cumprimento de suas atribuições legais, aplicam-se as disposições constantes da seção II do capítulo III desta lei, assim como as normas previstas em legislação específica, em especial na Lei nº 9.507, de 12 de novembro de 1997, na Lei n.º 9.784, de 29 de janeiro de 1999 e na Lei n.º 12.527, de 18 de novembro de 2011.



§ 4º Esta lei não se aplica aos bancos de dados mantidos exclusivamente para o exercício regular da atividade jornalística.

§ 5º Esta lei também não se aplica ao tratamento de dados pessoais:

I - realizado pelo Estado exclusivamente para fins de defesa nacional, investigação e repressão de infrações penais, inclusive quando envolverem transferência internacional de dados;

II - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

III - anônimos ou anonimizados.

§ 6º O dado pseudonimizado terá a mesma proteção dos dados pessoais, aplicando-se aos responsáveis pelo tratamento o disposto nesta lei.

Art. 3º Para os efeitos desta lei, considera-se:

I - anonimização: procedimento ou modificação destinada a impedir, de forma irreversível, a associação de um dado pessoal a um indivíduo identificado ou identificável ou capaz de retirar do dado tratado informação que possa levar à identificação do titular;

II - banco de dados: conjunto estruturado e organizado de dados pessoais, armazenado em um ou vários locais, em meio eletrônico ou não;

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

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

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

VI - consentimento: manifestação inequívoca, pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade específica;



VII - dado anônimo ou anonimizado: dado relativo a um titular que não possa ser identificado ou que, através de um processo de anonimização, não possa mais ser associado a uma pessoa natural identificada ou identificável;

VIII - dado pseudonimizado: dado que, através de um tratamento específico capaz de extrair um ou mais de seus elementos identificadores, não possa mais ser diretamente associado a um indivíduo, senão através do uso de informação adicional mantida separadamente em ambiente controlado e seguro;

VIII - dado pessoal: qualquer informação relacionada a pessoa natural identificada ou identificável;

IX - dado pessoal sensível: qualquer dado pessoal que revele a orientação religiosa, política ou sexual, a convicção filosófica, a procedência nacional, a origem racial ou étnica, a participação em movimentos políticos ou sociais, informações de saúde, genéticas ou biométricas do titular dos dados;

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

XI - interconexão: transferência de dados pessoais de um banco de dados a outro, mantido ou não pelo mesmo proprietário;

XII - operador: a pessoa natural ou jurídica contratada pelo responsável para o tratamento de dados pessoais;

XIII - responsável: a pessoa natural ou jurídica a quem competem as decisões referentes ao tratamento de dados pessoais;

XIV - titular: pessoa natural a quem se referem os dados pessoais objeto de tratamento nos termos desta lei;

XV - tratamento: qualquer operação ou conjunto de operações realizadas sobre dados pessoais ou banco de dados, com ou sem o auxílio de meios automatizados, tais como coleta, armazenamento, ordenamento, conservação, modificação, comparação, avaliação, organização, seleção, extração, utilização, bloqueio, cancelamento, anonimização, pseudonimização e fornecimento a terceiros, por meio de transferência, comunicação, interconexão ou difusão;

Parágrafo único. Considera-se privativo o uso das informações armazenadas no âmbito de organizações públicas ou privadas, respeitadas as



finalidades para as quais foi criado o banco de dados e observados os princípios e as garantias definidos nesta lei.

Art. 4º Ao tratamento de dados pessoais aplicam-se os seguintes princípios:

I - licitude, boa-fé e finalidade específica;

II - adequação, pertinência, integridade e atualização, periódica e de ofício, das informações;

III - conservação dos dados e identificação dos seus titulares apenas pelo período necessário às finalidades do tratamento;

IV - acesso do titular a informações sobre o tratamento de seus dados;

V - transparência no tratamento de dados, por meio inclusive da comunicação ao titular de todas as informações necessárias ao tratamento dos seus dados, tais como finalidade, forma de coleta e período de conservação, dentre outras;

VI - proporcionalidade no tratamento dos dados, sendo vedado o tratamento de dados que não seja adequado, necessário e proporcional à finalidade desejada ou que tenha fundamentado sua coleta;

VII - segurança da informação, por meio do uso de medidas técnicas atualizadas e compatíveis com os padrões internacionais, que sejam aptas a proteger os dados pessoais de destruição, perda, alteração, difusão, coleta, cópia ou acesso indevido e não autorizado;

VIII - prevenção, por meio da adoção de medidas técnicas adequadas para minimizar os riscos oriundos do tratamento de dados pessoais;

IX - responsabilização e prestação de contas pelos responsáveis e operadores que tratam dados pessoais, de modo a demonstrar a observância e o cumprimento das normas de proteção de dados pessoais;

X - o tratamento de dados pessoais deve ser compatível com as finalidades a que se destinam;

XI - limitação do tratamento dos dados pessoais ao mínimo necessário e indispensável para as finalidades para que são tratados;



XII - o desenvolvimento e a adoção de padrões técnicos e proporcionais de segurança da informação, entre os quais criptografia e pseudonimização, e de mecanismos que facilitem o controle dos titulares sobre seus dados pessoais desde a fase de concepção do produto ou do serviço até a sua execução;

XIV - a garantia da liberdade de expressão, de comunicação, de informação e de manifestação de pensamento, nos termos da Constituição Federal;

Parágrafo único. Excetua-se do disposto no inciso III a conservação de dados por órgãos e pessoas jurídicas de direito público ou realizada para fins históricos, estatísticos e científicos.

Dos Direitos do Titular

Art. 5º São direitos básicos do titular:

I - inviolabilidade da intimidade, da vida privada, da honra e da imagem;

II - indenização por dano material ou moral, individual ou coletivo;

III - recebimento de informações claras, completas e atualizadas sobre o tratamento de seus dados pessoais;

IV - consentimento, quando necessário;

V - o conhecimento dos principais elementos e critérios considerados para a tomada de decisão automatizadas a partir de seus dados pessoais, resguardado o segredo empresarial;

VI - cancelamento, a seu requerimento e ao término da relação entre as partes, dos seus dados pessoais em quaisquer bancos de dados, ressalvadas outras hipóteses legais;

VII - oposição ao tratamento dos seus dados pessoais, salvo quando indispensável para o cumprimento de obrigação legal ou contratual;



VIII - autodeterminação quanto ao tratamento dos seus dados, incluindo a confirmação da existência do tratamento de dados pessoais, o acesso aos dados, a correção gratuita de dados pessoais inverídicos, inexatos, incompletos ou desatualizados e o cancelamento de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta lei;

IX - a facilitação da defesa de seus direitos em processos judiciais ou administrativos, admitida a inversão do ônus da prova, quando, a critério do juiz, for verossímil a alegação ou, em se tratando de relação de consumo, for o consumidor hipossuficiente;

X - solicitação de revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem os interesses dos titulares.

XI - acesso a informações claras, completas e atualizadas, sobre o tratamento de seus dados pessoais, respeitados o segredo empresarial.

Parágrafo único. 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. 6º O titular poderá requerer do responsável o acesso à integralidade de seus dados pessoais, assim como a confirmação acerca do seu tratamento, bem como requerer, justificadamente, a elaboração de relatório que contenha todas as informações necessárias sobre o tratamento, tais como finalidade, forma de coleta e período de conservação.

§ 1º O requerimento do titular será atendido no prazo de até trinta dias, de forma gratuita, de maneira que a resposta seja de fácil compreensão.

§ 2º O armazenamento e tratamento dos dados pessoais serão realizados de forma a garantir o direito de acesso.

§3º Não será deferido o acesso a informações sobre tratamento de dados quando implicar violação de sigilo à investigação policial e ao segredo de justiça.

Art. 7º Sempre que constatar falsidade ou inexatidão nos dados pessoais coletados, o titular poderá requerer diretamente ao responsável a sua retificação sem qualquer ônus.

§ 1º O responsável deverá, de forma gratuita, no prazo de até trinta dias, corrigir os dados pessoais e comunicar o fato a terceiros que tenham tido acesso aos dados para que adotem igual procedimento.

§ 2º A comunicação a terceiros será dispensada caso seja comprovadamente impossível ou implique esforço desproporcional.

Art. 8º Caso os pedidos a que se referem os artigos 6º e 7º sejam manifestamente infundados ou excessivos, particularmente devido ao seu caráter recorrente, o responsável pelo tratamento pode:

a) exigir o pagamento de uma taxa razoável, tendo em conta os custos administrativos da retificação do dado pessoal, da comunicação ou da tomada das medidas solicitadas; ou

b) deixar de dar seguimento ao pedido.

Parágrafo único. Em qualquer caso previsto neste artigo, cabe ao responsável pelo tratamento demonstrar o caráter manifestamente infundado ou excessivo dos pedidos.

Art. 9º Constatado que o tratamento de dados se deu de forma inadequada, desnecessária, desproporcional, em contrariedade à finalidade que fundamentou sua coleta ou em violação a qualquer dispositivo desta lei, ou através da adoção de processo não autorizado de reversão de pseudonimização, o titular poderá requerer, sem qualquer ônus, o seu bloqueio, cancelamento ou anonimização, que será realizado pelo responsável no prazo de até trinta dias.

Art. 10. O legítimo interesse do responsável somente poderá fundamentar um tratamento de dados pessoais quando necessário para a realização de finalidade legítima e não afetar de forma concreta os direitos e liberdades fundamentais do titular.

Do Regime Jurídico do Tratamento de Dados Pessoais

Das Regras para Tratamento de Dados Pessoais



Art. 11. O tratamento de dados pessoais pode ser realizado nas seguintes hipóteses:

- I - mediante consentimento do titular;
- II - na execução de um contrato ou na fase pré-contratual de uma relação em que o titular seja parte;
- III - quando necessário para o cumprimento de obrigação legal pelo responsável;
- IV - quando realizado exclusivamente no âmbito da pesquisa histórica ou científica;
- V - quando necessário para tutela da saúde ou proteção da incolumidade física do titular ou de terceiro;
- VI - quando necessário para garantir a segurança da rede e da informação;
- VII - quando necessário para atender aos interesses legítimos do responsável pelo tratamento ou do terceiro a quem os dados sejam comunicados, desde que não prevaleçam sobre os interesses ou os direitos e liberdades fundamentais do titular dos dados; ou
- VIII - para o exercício regular de direitos em processo judicial ou administrativo.

§ 1º A autoridade competente poderá estabelecer medidas adicionais de segurança e de proteção aos dados pessoais sensíveis, que deverão ser adotadas pelo responsável ou por outros agentes do tratamento, ou solicitar a apresentação de relatório de impacto à privacidade.

§ 2º O tratamento de dados pessoais de acesso público deve ser realizado de acordo com os princípios desta lei, considerados a finalidade, a boa-fé e o interesse público que justificaram a sua disponibilização.

Art. 12. O consentimento do titular deve estar relacionado a uma finalidade legítima, sendo nulas as autorizações genéricas para o tratamento de dados pessoais.

§ 1º O consentimento do titular deve ser prestado de forma apartada de outros assuntos, em um formato inteligível e facilmente acessível, usando linguagem clara e simples.

§ 2º Se o tratamento para um fim diverso daquele para o qual os dados pessoais foram coletados não se baseia no consentimento do titular de dados, o responsável pelo tratamento deve, para assegurar-se de que o tratamento para outro fim seja compatível com a finalidade inicial da coleta, adotar medidas adequadas e compatíveis com os princípios e garantias desta lei, nos termos do regulamento, entre as quais técnicas de pseudonimização do dado.

Art. 13. O titular deve ter acesso a todas as informações relevantes acerca do tratamento dos seus dados, como finalidade, duração, identificação do responsável e suas informações de contato e terceiro a quem os dados forem comunicados.

§ 1º O ônus da prova acerca do consentimento e da sua adequação aos critérios legais cabe ao responsável pelo tratamento dos dados.

§ 2º O consentimento pode, a qualquer momento e sem ônus, ser revogado.

§ 3º Qualquer alteração relativa à finalidade, à duração, ao responsável ou a outro elemento relevante do tratamento de dados depende da renovação expressa e informada do consentimento pelo titular.

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

Art. 15. O tratamento de dados pessoais será encerrado:

I - ao fim do período consentido;

II - quando o tratamento não se mostrar mais adequado, necessário ou proporcional à finalidade a que se propõe ou que fundamentou sua coleta;

III - quando as medidas técnicas adotadas se mostrarem insuficientes para garantir a segurança e a qualidade da informação;



IV - mediante solicitação do titular, ressalvadas as demais previsões legais; ou

V - por decisão fundamentada de autoridade administrativa ou judicial, observadas as previsões do regulamento;

Parágrafo único. O encerramento implica o cancelamento ou anonimização dos dados pessoais do titular, ressalvadas as seguintes hipóteses:

I - cumprimento de obrigação legal ou decisão judicial;

II - pesquisa exclusivamente cultural, histórica ou científica, excetuadas as atividades ou hipóteses previstas no § 3º do art. 2º, em relação às quais esta lei não se aplica; ou

III - quando o titular expressa e inequivocamente consentir ou solicitar o contrário.

Art. 16. A comunicação e a interconexão de dados pessoais sujeitam todos aqueles que tiverem acesso aos dados às mesmas obrigações legais e regulamentares do responsável.

§ 1º. Os critérios adicionais para a comunicação e a interconexão de dados pessoais serão definidos em regulamento.

§ 2º Em caso de dano decorrente ou associado à comunicação ou à interconexão, respondem solidariamente todos aqueles que tiverem acesso aos dados.

Do tratamento de dados pessoais pelo poder público

Art. 17. O tratamento de dados pessoais pelas pessoas jurídicas de direito público e 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.

§ 1º O tratamento de dados no âmbito do Poder Público a que se refere esta lei tem por finalidade:



I - assegurar a adequada prestação de serviços públicos, simplificando a sua oferta e aperfeiçoando os procedimentos de atendimento aos usuários;

II - ampliar a efetividade na formulação, implementação, avaliação e monitoramento de políticas públicas;

III - instrumentalizar as atividades de regulação, fiscalização e controle.

§ 2º O tratamento de dados pessoais pelas pessoas jurídicas de direito público deve levar em consideração os incisos I, II, IV, VI, VII, VIII, IX, X, XI e XII, do Art. 4º, e os incisos I, II, III, VIII, IX, X e XI, do art. 5º, desta lei.

§ 3º A comunicação ou interconexão entre órgãos e entidades públicas de dados pessoais protegidos por sigilo fica condicionada ao consentimento expresso do usuário.

§ 4º Órgão ou entidade que recebam dados pessoais protegidos por sigilo por conta de processo de comunicação ou interconexão entre órgãos e entidades públicas ficarão responsáveis pela preservação dos sigilos, nos termos da legislação específica.

Art. 18. Os órgãos do Poder Público deverão informar as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre essas atividades em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos.

§ 1º Os órgãos do Poder Público que realizarem operações de tratamento de dados pessoais deverão indicar um encarregado.

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

Art. 19. Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, particularmente as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997, da Lei n.º 9.784, de 29 de janeiro de 1999 e da Lei n.º 12.527, de 18 de novembro de 2011.

Art. 20. 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 não estiverem atuando em regime de concorrência, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos desse Capítulo.

Art. 21. É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto quando houver previsão legal e 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 2011.

Parágrafo único. A transferência de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informada ao órgão competente e dependerá de consentimento do titular, exceto:

I - nas hipóteses de dispensa do consentimento previstas nesta lei;
OU:

II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do art. 17.

Art. 22. A comunicação de dados pessoais entre órgãos e entidades de direito público será objeto de publicidade.

Art. 23. 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. 24. O órgão competente poderá estabelecer normas complementares para as atividades de comunicação de dados pessoais.

Art. 25. Quando houver infração a esta lei em decorrência do tratamento de dados pessoais por órgãos públicos, o órgão competente poderá enviar informe com medidas cabíveis para fazer cessar a violação.



Parágrafo único. As punições cabíveis a agente público no âmbito desta lei serão aplicadas pessoalmente aos operadores de órgãos públicos, conforme disposto na Lei nº 8.112, de 11 de dezembro de 1990, e na Lei nº 8.429, de 2 de junho de 1992.

Art. 26. O órgão competente poderá solicitar a agentes do poder público a publicação de relatórios de impacto de privacidade e poderá sugerir a adoção de padrões e boas práticas ao tratamento de dados pessoais pelo poder público.

Da Segurança e Boas Práticas no Tratamento dos Dados

Art. 27. O responsável, o contratado e todos aqueles que tiverem acesso aos dados pessoais por comunicação, interconexão ou qualquer outra forma deverão:

I - adotar medidas técnicas de segurança e proteção dos dados atualizadas e compatíveis com os padrões internacionais, com a natureza dos dados tratados e com a finalidade do tratamento;

II - limitar seu uso à finalidade que gerou sua coleta; e

III - guardar sigilo em relação aos dados, observadas as hipóteses legais.

§ 1º O dever de sigilo permanece após o encerramento do tratamento.

§ 2º O responsável e o operador devem manter, por pelo menos cinco anos, registro das operações de tratamento de dados pessoais que realizarem, observada a regulamentação da autoridade competente.

Art. 28. O responsável deverá comunicar imediatamente à autoridade competente a ocorrência de qualquer incidente de segurança que exponha os dados armazenados e tratados ou que possa acarretar prejuízo aos titulares.

§ 1º O regulamento estabelecerá o conteúdo mínimo da comunicação.



§ 2º A pronta comunicação aos titulares afetados pelo incidente de segurança a que se refere o caput será obrigatória, independente de determinação da autoridade competente, nos casos em que coloque em risco a segurança pessoal do titular.

Art. 29. Os responsáveis pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, 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 outros aspectos relacionados ao tratamento de dados pessoais.

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

§ 2º As regras de boas práticas serão disponibilizadas publicamente e atualizadas e poderão ser reconhecidas e divulgadas pela autoridade competente.

Da Transferência Internacional de Dados

Art. 30. A transferência internacional de dados pessoais pode ser realizada nas seguintes hipóteses:

I - para países ou organizações internacionais que proporcionem nível adequado de proteção de dados, conforme decisão da autoridade competente;

II - quando o titular, após ser devidamente informado do caráter internacional do tratamento, consentir;

III - quando necessário para o cumprimento de obrigação prevista na legislação brasileira;

IV - quando necessário para tutela da saúde ou proteção da incolumidade física do titular ou de terceiro;



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

VI - quando a transferência for necessária para execução de política pública ou atribuição legal do serviço público;

VII - quando o responsável pela transferência, mediante autodeclaração, oferecer garantias de cumprimento dos princípios, dos direitos do titular e do regime jurídico de proteção de dados previstos nesta lei; e

VIII - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução criminal.

Art. 31. O grau de proteção de dados dos países de destino será analisado pela autoridade competente, por meio de critérios definidos em regulamento.

Art. 32. A transferência de dados pessoais para países que não proporcionem o mesmo grau de proteção de previsto nesta lei será permitida quando o responsável oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime jurídico de proteção de dados previsto nesta lei, na forma de cláusulas contratuais específicas para uma determinada transferência, de cláusulas contratuais padrão, de normas corporativas globais ou de selos, certificados e códigos de conduta e adequação emitidos por organismos de certificação qualificados ou pela própria autoridade competente nos termos do regulamento.

§ 1º Compete à autoridade administrativa competente ou a organismos de certificação qualificados prever requisitos, condições e garantias mínimas que deverão constar obrigatoriamente de cláusulas contratuais, que expressem os princípios gerais da proteção de dados, os direitos básicos do titular e o regime jurídico de proteção de dados.

§ 2º A autoridade administrativa competente ou organismos de certificação qualificados poderão aprovar e atestar a adequação a normas corporativas globais dos responsáveis pelo tratamento de dados que fizerem parte de um mesmo grupo econômico, dispensando a autorização específica para determinado tratamento, desde que observadas as garantias adequadas para a proteção dos direitos dos titulares dados pessoais.



SEÇÃO V

Da Responsabilidade

Art. 33. Aquele que efetuar o tratamento de dados pessoais responderá, no limite de sua atuação, pela reparação dos danos causados aos titulares ou terceiros, se, no exercício de sua atividade, não tiver cumprido as determinações desta lei ou da autoridade competente que lhe são impostas.

Parágrafo único. Os agentes envolvidos na mesma atividade de tratamento de dados que provocarem dano ao titular responderão solidariamente por sua reparação, assegurado o direito de regresso contra dos demais àquele que reparar integralmente o dano.

Art. 34. Na aplicação dos princípios indicados nos incisos IX e X, do art. 4º, desta lei, o responsável deverá:

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;



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

II - estar preparado para demonstrar a efetividade de seu programa de governança de privacidade quando apropriado, e em especial, a pedido de autoridade competente 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.

Parágrafo único. Requisitos mínimos e procedimentos referentes ao programa de governança em privacidade serão estabelecidos em regulamento, observada a estrutura, escala e volume das operações, bem como a sensibilidade dos dados tratados, a probabilidade e a gravidade dos danos para os titulares dos dados.

Da Tutela Administrativa

Art. 35. A União fiscalizará o cumprimento desta lei, apenando eventuais infrações mediante processo administrativo que assegure o contraditório e a ampla defesa.

Art. 36. A autoridade competente designada para zelar pela implementação e pela fiscalização desta será juridicamente condicionada pelos princípios da legalidade, celeridade, finalidade, razoabilidade, proporcionalidade, impessoalidade, igualdade, devido processo legal, publicidade e moralidade e terá as seguintes atribuições:

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

II - fiscalizar o tratamento de dados pessoais e processos envolvidos com dados pessoais visando garantir a sua conformidade aos princípios e regras desta lei, mediante processo administrativo que assegure o contraditório e a ampla defesa;

III - promover o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e as medidas de segurança;

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



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

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

VII - dispor sobre as formas pelas quais se dará a publicidade das operações de tratamento;

VIII - solicitar, a qualquer momento, ao Poder Público, informações acerca dos seus órgãos que realizem operações de tratamento de dados pessoais, informe específico sobre o âmbito, natureza dos dados e outras informações relacionadas ao tratamento realizado, podendo emitir parecer técnico complementar para garantir o cumprimento desta lei;

IX - elaborar relatórios anuais acerca de suas atividades e sobre o estado da proteção de dados pessoais no país;

X - realizar demais ações dentro de sua esfera de competência, inclusive as previstas nesta lei e em legislação específica; e

XI - editar normas complementares para a proteção de dados pessoais.

Parágrafo único. No exercício das atribuições previstas neste artigo, a autoridade competente deverá zelar pela preservação do segredo empresarial e do sigilo das informações, quando assim atribuído em lei, sob pena de responsabilidade.

Art. 37. Aquele que infringir o disposto esta lei, fica sujeito, conforme o caso, às seguintes sanções administrativas, sem prejuízo daquelas de natureza civil, penal e das definidas em normas específicas:

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

II - alteração, retificação, bloqueio ou cancelamento dos dados;

III - multa de até 2% sobre o faturamento da empresa ou do grupo econômico no Brasil no seu último exercício, excluídos os tributos, por infração, no caso de reincidência de infração cometida que leve à aplicação das penalidades dos itens I e II;



IV - suspensão parcial ou total das atividades específicas de tratamento de dados pessoais;

V - proibição parcial ou total das atividades específicas de tratamento de dados pessoais;

§ 1º As sanções previstas neste artigo serão aplicadas pela autoridade competente referida no caput do art. 35, podendo ser aplicadas isolada ou cumulativamente, inclusive por medida cautelar antecedente ou incidente de procedimento administrativo.

§ 2º Apenas medidas cautelares urgentes poderão ser tomadas antes da defesa.

§ 3º A autoridade competente poderá notificar o responsável, o contratado e todos aqueles que tiverem acesso aos dados pessoais para, sob pena de desobediência, prestarem informações acerca do tratamento de dados, resguardado o segredo empresarial.

§ 4º A pena de proibição de tratamento de dados pessoais não será superior a cinco anos.

Art. 38. Na aplicação das penas estabelecidas nesta lei, levar-se-á em consideração o princípio da proporcionalidade, bem como:

I - a gravidade da infração;

II - a boa-fé do infrator;

III - a vantagem auferida ou pretendida pelo infrator;

IV - a situação econômica do infrator;

V - a reincidência;

VI - o grau de lesão;

VII - a cooperação do infrator;

VIII - a adoção de mecanismos e procedimentos internos capazes de minimizar a lesão;



IX - a implementação de padrões e medidas de boas práticas, nos termos desta lei;

X - o cumprimento ou não do disposto no art. 28 desta lei pelo infrator; e

XI - se o dano decorreu da transferência de dados pessoais para países que não proporcionaram o mesmo grau de proteção previsto nesta lei.

Art. 39. Em qualquer fase do processo administrativo, a autoridade competente poderá adotar medida preventiva, quando houver indício ou fundado receio de que o agente possa causar lesão irreparável ou de difícil reparação, ou torne ineficaz o resultado final do processo, fixando prazo para seu cumprimento e o valor da multa diária a ser aplicada, no caso de descumprimento.

Art. 40. O pagamento da multa ou o cumprimento da obrigação de fazer ou não fazer de empresa responsável sediada no exterior pode ser exigido da filial, agência, sucursal, estabelecimento ou escritório instalado no Brasil.

Art. 41. A decisão final da autoridade competente, cominando multa ou impondo obrigação de fazer ou não fazer, constitui título executivo extrajudicial.

Disposições Finais e Transitórias

Art. 42. As normas de prevenção e repressão às infrações contra a ordem econômica são aplicáveis ao tratamento dos dados pessoais, nos termos da legislação específica, observada a competência da autoridade de defesa da concorrência.

Art. 43. Os direitos previstos nesta lei não excluem outros decorrentes de tratados ou convenções internacionais de que o Brasil seja signatário ou da legislação interna ordinária.

Art. 44. Ficam revogadas as disposições em contrário, inclusive os incisos VII, VIII, IX e X do art. 7º da Lei nº 12.965, de 23 de abril de 2014.

Art. 45. A autoridade 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. 46. As atividades, atribuições e competências estabelecidas à autoridade competente a que se refere esta lei serão exercidas por órgão do Ministério da Ciência, Tecnologia, Inovações e Comunicações, em caráter transitório, até que o Poder Executivo venha a constituir entidade destinada a essa finalidade.

Art. 47. Esta lei entra em vigor após decorrido trezentos e sessenta e cinco dias de sua publicação oficial.

Sala da Comissão,

, Presidente

, Relator



SF/18051.14988-53