PARECER Nº , DE 2018

De PLENÁRIO, em substituição às COMISSÕES DE ASSUNTOS ECONÔMICOS E DE CONSTITUIÇÃO, JUSTIÇA E CIDADANIA, 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

Vêm ao exame deste Plenário 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 unânime daquela Comissão, inclusive incorporando emendas apresentas 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 dos seguintes convidados: Luis Felipe Salin Monteiro, Secretário da Tecnologia da Informação e Comunicação do Ministério do Planejamento, Desenvolvimento e Gestão; João Gomes Cravinho, Embaixador da União Europeia no Brasil; Maximiliano Martinhão, Conselheiro do Comitê Gestor da Internet no Brasil; Dr. Rony Vainzof, Diretor do Departamento de Defesa e Segurança da Federação das Indústrias do Estado de São Paulo - FIESP; Bruno Bioni, Pesquisador da Rede Latino-Americana de Estudos sobre Vigilância, Tecnologia e Sociedade - LAVITS; Dr. Marcio Cots, Advogado especialista; Mario Viola de Azevedo Cunha, Consultor e especialista em privacidade e proteção de dados pessoais; e João Emílio Padovani Gonçalves, Gerente-Executivo de Política Industrial da Confederação Nacional da Indústria - CNI.

Esta relatoria reuniu-se, ainda, com mais de 100 grupos e pessoas interessadas no debate em torno deste Projeto de Lei, no último dia 22, ocasião em que foram ouvidos todos os que desejaram expor suas considerações.

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

O Plenário desta Casa aprovou, no dia 24 último, requerimento de urgência subscrito pelos Senhores Líderes de diversas bancadas.

Ao total, foram ainda apresentadas, perante a Comissão de Assuntos Econômicos, 32 Emendas ao PLS e 14 subemendas à Emenda

Substitutiva nº 31 – CCT/CMA, de autoria de diversos Senhores Senadores. Também veio protocolada a Emenda nº 57, de Plenário.

Nada mais há que se relatar.

II – ANÁLISE

II.1. Cenário internacional:

A matéria é de extrema relevância para o País e o debate, cada vez mais urgente, sobretudo em razão da entrada em vigor, no último dia 25, do Regulamento Geral de Proteção de Dados, da União Europeia.

No Brasil, apesar de nossa Constituição cidadã prever instrumentos e mecanismos para a preservação da intimidade e da privacidade do cidadão, não temos uma efetiva proteção prevista em normas infraconstitucionais. O que há, em nosso País, são regras frágeis, dispersas em várias leis, o que não contribui para um sistema eficaz.

E esse não é um debate recente no mundo.

Desde 1948, a Declaração Universa de Direitos Humanos já endossava, entre os direitos inalienáveis do homem, a proteção à privacidade do indivíduo e de sua família. Em 1950, A Convenção Europeia de Direitos Humanos replicou essa mesma proposta da Organização das Nações Unidas (ONU).

Porém, com o advento da informática e das tecnologias da informática, em especial a internet, o mundo passou a compreender que as informações coletadas do indivíduo – seja por empresas, seja por Governos – tinham correlação direta com sua privacidade.

Privacidade e dados pessoais, portanto, passaram a ser elementos inseparáveis um do outro.

Foi com essa visão que, em 1980, a Organização para a Cooperação e o Desenvolvimento Humano (OCDE) adotou as “Diretrizes sobre

a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais", um passo importante na direção da harmonização das legislações nacionais.

Em 1981, foi a vez do Conselho da Europa editar a "Convenção para a Proteção de Indivíduos com Relação ao Processamento Automático de Dados Pessoais", o primeiro documento internacional com força legal disciplinando especificamente essa temática, aberto a membros e não membros da Comunidade Europeia.

Daí para frente, uma sucessão de tratados e documentos internacionais passaram a legitimar a cultura da proteção da privacidade, entre as quais a Diretiva 95/46, do Parlamento e do Conselho Europeus, e o Sistema de Regras de Privacidade Transfronteiriça da Cooperação Econômica Ásia-Pacífico (APEC).

Mais recentemente, em 2016, a União Europeia implementou a Regulação 2016/679 (Regulamento Geral de Proteção de Dados), que, como dissemos, entrou em vigor no último dia 25.

Esse breve histórico internacional revela uma visão fundamental para países em desenvolvimento, como o Brasil: sociedades civilizadas já perceberam que a proteção da privacidade é elemento intrínseco à dignidade da pessoa humana, de tal forma que qualquer ação capaz de afetar a intimidade do cidadão é também uma afronta a uma vida digna.

II.2. A importância da proteção dos dados pessoais:

Lamentavelmente, no Brasil, não temos ainda a cultura da proteção dos dados pessoais. Temos uma noção ainda superficial da importância da intimidade. Porém, não buscamos associar diretamente o tratamento dos dados pessoais com a privacidade.

A falta dessa noção tem-nos impedido de avançar em um debate sério e eficaz sobre uma lei ampla de proteção de dados

Um observador menos atento poderia levantar o seguinte questionamento: por que tanta importância atribuída à necessidade de um marco regulatório de proteção de dados?

A resposta, porém, é simples: o dado pessoal é, hoje, o principal insumo da economia globalizada e baseada em tecnologia.

E é preciso desmistificar o ideário popular: dado pessoal não é utilizado apenas por empresas digitais responsáveis por aplicativos e redes sociais: todos os setores econômicos, sem exceção, processam dados. E, dentre esses, estão dados pessoais de consumidores, funcionários, parceiros comerciais, prestadores de serviço ou de fornecedores.

E, cada vez mais, dados são processados e valorados economicamente: vivemos a era da economia dirigida por dados[1].

O nível de avanço tecnológico a que a humanidade chegou permite o processamento massivo de dados, baseado em tecnologia digital avançada. E esse processamento já ocorre com base em inteligência artificial e algoritmos complexos, capazes de influenciar a vida do cidadão.

Podemos não ter consciência disso, mas tudo o que fazemos é coletado e armazenado em bases de dados cada vez maiores: ao acordarmos, usamos o celular (smartphone), tablet ou relógio inteligente (smartwatch) para as atividades cotidianas, como verificar mensagens, ler notícias na internet, conferir o clima e o nível de trânsito até o trabalho ou escola.

Ao sair de casa, as torres de telefonia celular registram nosso itinerário. Aplicativos baseados em geolocalização monitoram nossos passos e traçam nossas rotas do dia a dia. Programas instalados em nossos carros, telefones ou computadores registram nossos hábitos, gostos e preferências.

Há aqueles que monitoram com quem falamos por ligações telefônicas, videochamada ou mensagens de texto registrando data, hora e duração da chamada. Às vezes, até o conteúdo.

Nosso cartão de crédito revela nossos hábitos financeiros e nosso próprio consumo e como isso nos define: preferência gastronômica, roupas e

[1] *Data-driven economy.*

vestuário, hábitos de lazer, preferências ideológicas, opinião política, crença religiosa e até mesmo nossa vida sexual.

Tudo é mensurável em dados, que podem revelar quem somos.

O dado pessoal é, também, um importante elemento para a concretização de políticas públicas e o exercício de funções e atividades de interesse público, dado o elevado grau de informatização e sistematização do Estado brasileiro.

Por isso, regras claras são fundamentais para assegurar a conformidade e o impulsionamento da atividade econômica influenciada por um cenário global de confiança do cidadão, quanto ao respeito a direitos fundamentais que lhes são caros.

II.3. Reflexos do tratamento de dados pessoais:

O processamento massivo de dados, inclusive pessoais, constitui um elemento essencial de qualquer empresa ou governo atualmente, sobretudo em razão da crescente automatização de suas atividades e processos.

E, para auxiliar na tomada de decisões e na solução de problemas complexos, próprios da atividade econômica, são necessários sistemas de análise de dados capazes de realizar estimativas e recomendações simples e objetivas, o que amplia a eficiência de empresas, proporcionando inovação, maior qualidade de vida e produtos e serviços mais seguros e confiáveis. O progresso tecnológico também aquece a economia, ampliando postos de trabalho, permitindo maior e melhor qualificação de trabalhadores e transformando negócios e a própria sociedade.

Ao longo desta relatoria, ouvimos diversas empresas, associações e representantes da sociedade civil, que trouxeram contribuições impressionantes sobre como a utilização responsável de dados pessoais pode expandir negócios e impulsionar a economia.

Para ilustrar esses relatos, podemos citar um exemplo de um laboratório farmacêutico brasileiro.

O acesso a medicamentos é uma das maiores preocupações, tanto para o Governo, como para as empresas do setor. Somente no Brasil, temos 72 mil farmácias e menos de 17% desse total pertencem a redes: vale dizer, 83% desse quantitativo é formado por pontos de venda independente.

Como todos sabem, a Receita Federal disponibiliza, em seu site na internet, um portal de consultas de dados cadastrais de pessoas jurídicas, que são de acesso público, para maior segurança do cidadão. Com base nessas informações, foi possível identificar cerca de 30 mil farmácias e drogarias em regiões afastadas, distribuídas em mais de 21 mil cidades que não eram atendidos pela rede de distribuição de medicamentos. A partir dessa análise, esse laboratório passou a abastecer farmácias e drogarias estabelecidas nesses municípios levando medicamentos importantes para a população.

Estamos testemunhando a recente crise de distribuição de combustível no País. O episódio serviu para demonstrar como nossa economia depende do sistema rodoviário para transporte de produtos, inclusive de combustível, um insumo essencial para o bom funcionamento da sociedade brasileira.

Objetivando a melhoria na rede de distribuição, uma grande empresa do setor mapeou a localização de pontos de abastecimento, a partir da utilização de informações publicamente acessíveis no Cadastro Nacional de Atividades Econômicas (CNAE). Com base nesses dados, foi possível analisar a capacidade dos tanques de cada ponto de abastecimento, inclusive por tipo de combustível, e direcionar, de forma constante, a oferta e a entrega desse insumo de acordo com as necessidades da região.

E não apenas isso: cruzando informações de alterações do Quadro de Sócios e Administradores (QSA), inclusão em Dívida Ativa e Lista de Empresas Idôneas e Suspensas, a empresa conseguiu identificar postos fraudadores.

Mais ainda: não é somente o setor privado que se beneficia do processamento de dados.

O Estado possui valores bastante significativos em créditos a serem recebidos por contribuintes inadimplentes. Uma das maiores dificuldades,

nesse sentido, para as Procuradorias fazendárias, é justamente cobrar esses valores, principalmente em razão da dificuldade de localizar bens.

Com base no cruzamento de diversas fontes de dados públicos, a Procuradoria de determinado município conseguiu obter o endereço único e atualizado de diversos devedores que constavam de lista de créditos já cobrados e não pagos. Com isso, as cobranças se tornaram mais eficientes e houve um retorno imediato de recursos financeiros para o Poder Público.

E não somente isso: acessando dados disponibilizados publicamente pela Receita Federal, foi possível comprovar fraudes dos devedores, como a transferência de ativos para empresas do mesmo grupo econômico.

Ainda no âmbito do Poder Público, o processamento de dados pode contribuir para evitar fraudes em licitações, seja identificando a correlação entre empresas supostamente concorrentes, seja rejeitando garantias incompatíveis com o porte da licitação.

Além disso, o Poder Público conseguiu utilizar dados públicos da Receita Federal para comprovar fraudes dos devedores, como transferência para empresas do mesmo grupo econômico. Além disso, foram evitadas fraudes em licitações, seja identificando correlação entre empresas “concorrentes”, seja rejeitando garantias incompatíveis com o porte da licitação.

II.4. Situação da proteção de dados no Brasil:

Não é correto afirmar que o Brasil carece de normas de proteção da privacidade ou de dados. Não temos uma lei geral, mas nosso sistema legal dispõe de leis setoriais, que tratam, insuficientemente, da proteção de dados pessoais.

Dentre elas, podemos citar a Lei de Registros Públicos[2], o Código de Defesa do Consumidor[3], a Lei do Habeas Data[4], o Código Civil brasileiro[5], a

[2] LEI Nº 6.015, DE 31 DE DEZEMBRO DE 1973.
[3] LEI Nº 8.078, DE 11 DE SETEMBRO DE 1990.
[4] LEI Nº 9.507, DE 12 DE NOVEMBRO DE 1997.
[5] LEI Nº 10.406, DE 10 DE JANEIRO DE 2002.

Lei do Cadastro Positivo[6], a Lei de Acesso à Informação[7], o Marco Civil da Internet[8], entre outras. A matriz, porém, da proteção de dados, é a Constituição federal, que reserva numerosas disposições sobre a preservação da intimidade, da honra e da imagem do cidadão, inclusive a partir do *status* de direito fundamental (art. 5º, inc. X e XII).

E parte desse ordenamento jurídico surgiu a partir de uma visão do Governo federal para efetivação do tripé regulatório de dados no Brasil:

1. a regulamentação do acesso à informação pública;

2. a regulação do uso da internet no Brasil; e

3. a edição de um marco geral de proteção de dados pessoais, que ora promovemos.

O Brasil já dispõe da Lei de Acesso à Informação e do Marco Civil da Internet. Precisamos, agora, concluir o processo legislativo da Lei Geral de Proteção de Dados Pessoais - LGPD, para que o País entre 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

---

[6] LEI Nº 12.414, DE 9 DE JUNHO DE 2011.

[7] LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011.

[8]

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 necessidade urgente de aprovação desta lei e, mais ainda, de definição acerca da criação de uma autoridade central de proteção de dados pessoais.

O Poder Executivo, a seu turno, já se posicionou, seja pelo encaminhamento do Projeto de Lei nº 5.276, de 2016, agora em trâmite na Câmara dos Deputados, seja pelo lançamento da Estratégia Brasileira para a Transformação Digital (E-Digital), no último dia 22/03/2018.

Segundo o documento oficial, disponível na internet, "a E-Digital oferece um amplo diagnóstico dos desafios a serem enfrentados, uma visão de futuro, um conjunto de ações estratégicas que nos aproximam dessa visão, e indicadores para monitorarmos o progresso no atingimento de nossos objetivos". Consta, ainda, de suas recomendações, a edição de uma lei geral de proteção de dados.

E é o que estamos a produzir neste momento.

II.5 Emendas apresentadas:

Foram apresentadas **25 Emendas** ao PLS 330, de 2013, e **15 Subemendas à Emenda Substitutiva nº 31**, aprovada na Comissão de Ciência e Tecnologia e na Comissão de Meio Ambiente, perante a Comissão de Assuntos Econômicos. Em razão do regime de urgência, foram apresentadas, ainda, em Plenário, **2 Emendas**, que agora passamos a analisar.

1. **SUBEMENDA 01**: excepciona, da incidência normativa da lei, os bancos de dados das serventias notariais e de registro;

2. **SUBEMENDA 02**: delineia regras específicas de tratamento de dados pessoais quando voltadas a registros em cadastros de crédito negativadores;

3. **EMENDA 32**: prevê regras específicas para inclusão de dados restritivos ao crédito em decorrência de dívida.

Somos pela **rejeição** das três sugestões apresentadas pela **Senadora Marta Suplicy**, pois 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. A esse respeito, inclusive, estamos alinhados com as diretrizes de mínimas excepcionalidades da lei.

4. **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;

5. **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. Assemelha-se à **EMENDA 47**, que acolhemos em parte também.

6. **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.

Votamos pela **aprovação** dessas subemendas apresentadas pelo **Senador José Medeiros**.

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. Também ampliamos as hipóteses de transferência internacional de dado, para incorporar instrumentos modernos de regulação, presentes tanto no Sistema de Regras de Privacidade Transfronteiriça da Cooperação Econômica Ásia-Pacífico (APEC), como no Regulamento Geral de Proteção de Dados da União Europeia.

Com relação as normas incidentes sobre o tratamento de dados pessoais de crianças e adolescentes, entendemos **acatada parcialmente**, na medida em que simplificamos sua redação com relação ao texto aprovado pela CCT, mas conjugamos com o conteúdo das **EMENDAS 35 e 49**, respectivamente do Senador Humberto Costa e da Senadora Lídice da Mata, aqui **acatadas** em grande parte para ampliar a proteção da criança.

7. **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.

Compreendemos o intuito da proposta e votamos por sua **aprovação parcial**, muito embora com uma redação mais apropriada para o que se pretende, na forma do Substitutivo ora proposto. Limitamos o conceito para prever informações médicas e de tratamento de saúde e diagnóstico sobre o estado físico ou psíquico do titular dos dados.

8. **SUBEMENDA Nº 7:** delimita em 15 dias corridos o prazo para o responsável pelo tratamento dos dados corrigir e comunicar a retificação dos dados.

9. **SUBEMENDA Nº 8:** estabelece prazo de 15 dias **úteis** para providências imediatas requeridas pelo titular dos dados em caso de imprecisão das informações.

Ambas subemendas foram apresentadas pela nobre Senadora Vanessa Grazziotin e merecem **acolhida parcial**. Ouvimos os apelos que nos foram direcionados, tanto por parlamentares, como por representantes da sociedade civil e do setor empresarial, e fixamos todos os prazos administrativos em 10 dias úteis, harmonizando com o que dispõe o CDC.

Porém, criamos regra transitória, para que, no primeiro ano de vigência da lei, tais prazos sejam de 30 dias corridos. É preciso compreender que o Brasil enfrentará, pela primeira vez, um sistema regulatório complexo e muito subjetivo, de maneira que buscamos equilibrar os interesses sociais em discussão.

10. **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 parcial**, conforme o Substitutivo, na medida em que propomos um regime próprio de responsabilidade civil, alinhado à proposta apresentada também pela Senadora Lídice da Mata, através da **EMENDA 52**, com igual acolhida.

A esse respeito, porém, importante detalhar que não compactuamos apenas com um ponto dentre os componentes desta última emenda acolhida da Senadora representante do Estado da Bahia: a incursão do regime de responsabilidade civil solidária e objetiva do CDC.

O texto proposto importa do CDC a integralidade do regime de responsabilidade nas relações de consumo. Ora, a proteção de dados pessoais não se dá apenas nas relações de consumo, mas, como já dissemos, aplica-se aos dados de qualquer pessoa natural, em qualquer ambiente social ou relação jurídica (salvo aquelas excepcionadas na própria Lei).

Daí que não é razoável que a proteção de dados de consumidores seja menos ou mais valiosa que a proteção de dados de funcionários, fornecedores, membros de uma associação, de uma congregação religiosa ou política ou condôminos de um edifício residencial ou comercial, onde inexiste relação de consumo. Além disso, o Substitutivo acolhe grande parte das reivindicações de todos os setores da sociedade, mas em uma dosagem de equilíbrio. No mais, a redação sugerida na emenda atrai insegurança jurídica e não se compactua com a melhor técnica legislativa.

11. **SUBEMENDA Nº 10**: versa sobre maior escopo de proteção dos dados pessoais sensíveis. Somos por sua **aprovação parcial**. De fato, estamos convencidos de que o tratamento de dados pessoais sensíveis deva possuir balizas rigorosas mínimas prevista em lei, para além de normas complementares que a autoridade administrativa vier a editar. Entre essas regras, limitamos as hipóteses que autorizam o tratamento de dados pessoais sensíveis, além de especificar e qualificar melhor a forma de consentimento, para que passe a ser também específico e expresso. Nesse sentido, aliás, conjugamos essa subemenda à **EMENDA 33** (Senador Humberto Costa) e à **EMENDA 50** (Senadora Lídice da Mata), também acolhidas quase e sua totalidade.

12. **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, quanto aos dados pseudonimizados, sobre os quais iremos discorrer mais à frente.

13. **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.

14. **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 **aprovação**, atendendo aos apelos da sociedade civil.

15. **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.

16. **EMENDA Nº 34:** amplia as hipóteses de penalidades administrativas, para incluir a publicização da infração pela autoridade central, o bloqueio e a eliminação de dados pessoais. Estamos **acolhendo parcialmente** a proposta, especialmente no que tange a proposta de tornar públicas as infrações, porém, na forma do Substitutivo. Isso porque a autoridade central já detém essa atribuição, na medida em que poderá editar normas complementares a respeito de suas atividades, e, uma vez findo processo administrativo sancionador, que tem natureza pública, parece evidente que a autoridade central tornará pública sua decisão de penalizar aquele que comete infrações, após o exercício do contraditório e do devido processo legal.

17. **EMENDA Nº 36:** a proposta veda o tratamento de dados pessoais quando houver vício de consentimento, erro, dolo, coação, estado de perigo ou simulação, além de considera-nulo. Somos por sua **rejeição**. Ora, o Substitutivo deixa claro que o consentimento, quando necessário, deverá ser livre, informado e inequívoco e, no caso de dados pessoais sensíveis, ainda expresso e específico. Não há como se admitir que o consentimento dado, com tais qualificadoras, tenha sido viciado. Ademais, as regras acerca da manifestação da vontade previstas no Código Civil complementam esta Lei, especialmente quando à natureza jurídica do consentimento dado e a validade dos negócios jurídicos nele baseados.

18. **EMENDA Nº 37:** o texto sugere que o escopo da lei seja aplicado à “proteção de dados pessoais”, e não da “proteção da pessoa natural com relação ao tratamento de seus dados pessoais”. Discordamos dessa visão. Ouvimos renomados especialistas, com formação acadêmica sólida, que sustentaram exatamente o contrário, tal como estamos propondo em nosso Substitutivo. Somos, assim, por sua **rejeição**. No entanto, com o objetivo de simplificar a comunicação em torno da matéria, optamos por fazer referências, no relatório, à expressão “proteção de dados pessoais”, mais objetiva e direta.

19. **EMENDA Nº 38:** propõe a exclusão das exceções aplicáveis ao poder público. Atendemos a apelos da sociedade civil e do próprio Governo e reequilibramos essa questão, para minimizar as hipóteses de exclusão da lei. Da forma como propomos, estamos remetendo alguns direitos do cidadão, no tratamento de dados pessoais pelo setor público, à disciplina da Lei de Acesso à Informação, já em vigor e bastante testada pela sociedade. **Acolhida em parte**.

20. **EMENDA Nº 39:** a emenda sugere a edição de lei específica para disciplinar as atividades de tratamento de dados para defesa nacional, segurança pública, investigação penal, improbidade administrativa e atividades de inteligência, observadas as regras gerais e princípios desta Lei. Somos por sua **acolhida**.

21. **EMENDA Nº 40**: sugere um direito, além dos já previstos, no sentido de que o tratamento de dados pessoais no exercício regular de direito não pode ser usado contra o titular dos dados. **Acolhemos, em parte**. Optamos pela redação anteriormente sugerida pelo parecer da CCT, em que se consagrou o princípio de não discriminação ilegítima.

22. **EMENDA Nº 41:** remete as reclamações sobre infrações a esta Lei ao PROCON de cada Estado federativo. Somos por sua **rejeição**, com firme convicção. Como já dissemos, a proteção de dados pessoais não deve ser limitada às

relações de consumo, daí não ser minimamente razoável que criemos um regime peculiar para a disciplina de tratamento de dados pessoais para determinadas categorias de relações jurídicas.

23. **EMENDA Nº 42:** de autoria do nobre Senador Lindbergh Farias, propõe uma qualificação mais detalhada para o consentimento. Somos por sua **acolhida**.

24. **EMENDA Nº 43:** apresenta uma proposta de solução para um problema que reputa recorrente no âmbito do sistema de acesso à informação. Somos por sua **rejeição**. O projeto de proteção de dados pessoais não é a plataforma adequada para dirimir controvérsias ou soluções para um sistema distinto.

25. **EMENDA Nº 44:** propõe que a autoridade competente deva criar instrumentos simplificados, inclusive pela internet, para receber reclamações e denúncias. Somos por sua **aprovação**, na forma do Substitutivo.

26. **EMENDA Nº 45:** aumenta o teto para aplicação da multa para 5% sobre o faturamento bruto da empresa ou grupo econômico no Brasil, por infração. Com isso, a Emenda busca suprimir a reincidência como condição da multa, tal como sugerimos anteriormente. Somos por sua **acolhida parcial**. Discordamos apenas do percentual sugerido e da circunstância unitária do cometimento da infração. Mantemos, porém, em 2% sobre o faturamento da empresa ou do grupo econômico, no Brasil.

27. **EMENDA Nº 46:** apresenta uma disciplina mais abrangente para o legítimo interesse, que **acolhemos em parte**. Concordamos que o legítimo interesse deva ser utilizado, pelas empresas, com base em uma finalidade legítima e baseada em uma situação concreta, observados os direitos e princípios desta lei. Porém, ao invés de tornarmos obrigatória a emissão de relatório de impacto sobre a privacidade, o que poderia ser um ônus desproporcional a

empresas de menor porte, especialmente *startups*, estamos remetendo a questão à autoridade central, que terá condições de avaliar em que medida esse documento deva ser imposto e elaborado. Com isso, conjugamos essa emenda ao texto da **EMENDA 51**, do Senador Lindbergh Farias, e da **EMENDA 53**, da Senadora Lídice da Mata, sem, contudo, detalhar na lei todos os elementos e circunstâncias do relatório sugerido, na medida em que essa é matéria típica de regulamento.

28. **EMENDA Nº 48:** resolve uma omissão sistemática, quando ao tratamento de dados pelos serviços notariais e de registro. Somos por sua **aprovação parcial**, submetendo os cartórios à disciplina do setor público, a despeito de sua natureza privada. Vai na direção, ainda, da **EMENDA 57,** do nobre Senador Telmário Mota, ora **rejeitada**.

29. **EMENDA Nº 54 A 56:** buscam qualificar o tipo de pesquisa histórica ou científica de que trata o projeto, para contemplar aquelas de evidente interesse público ou geral, sem fins lucrativos. Somos por sua **rejeição**. Ora, a pesquisa histórica ou científica com fim lucrativo também deve ser preservada, não sendo legítimo direcionar menor grau de proteção de dados apenas para aquelas realizadas sem finalidade lucrativa.

II.6 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 reclamos da sociedade civil.

Buscamos ouvir, em reunião aberta, mais de 100 especialistas, acadêmicos, membros do Ministério Público, das Polícias Civil e Federal, de associações e de empresas.

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 reconhecermos sua relevância para o mundo. A RGPD entrou 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 menoscabar 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, considerando os esforços razoáveis que uma empresa possa utilizar para reverter o dado para um dado de pessoa identificada ou identificável. Dessa forma, a anonimização será aquele procedimento de dissociação da identidade de um indivíduo, na medida em que a empresa responsável tenha menores condições e custos econômicos, financeiros e tecnológicos para proceder à reversão do processo.

Por outro lado, se os dados, por qualquer razão, podem ser revertidos e reidentificados com facilidade, então estamos a tratar de dados pseudonimizados[9], um conceito moderno apresentado pela RGPD, que inspira maior segurança no tratamento. Além disso, o dado pseudonimizado reclama incentivos, dado seu grau maior de proteção, o que propomos ao longo do texto, que é o que buscamos fazer.

Optamos, 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,

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

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 aa 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 doa 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, mas suficientes, como base legal de tratamento de dados. Optamos por retomar o rol exemplificativo de atividades que poderiam ser compreendidas como legítimo interesse, mas com uma redação que não deixe margem de dúvida tratar-se de rol não taxativo.

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, por decreto, evidencie quem exercerá as atribuições desse órgão.

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.

Quanto à aplicabilidade da norma, foi ampliado o rol de exceções, para comportar, ainda, a segurança pública, atividades de inteligência do País (Lei 9.883/90); e apuração de improbidade administrativa, para além da atividade jornalística, defesa nacional e investigação penal.

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, 7, 8, 9, 10, 11, 13 e 14** e das **Emendas nºs 33, 34, 35, 38, 39, 40, 42, 44, 45, 46, 47, 48, 49, 50, 51, 52 e 53**, 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 – PLEN (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 pessoais, tendo como fundamentos:

I - a dignidade da pessoa humana;

II - a autodeterminação informativa;

III - a liberdade de expressão, de comunicação e de opinião;

IV - a inviolabilidade da intimidade, da vida privada, da honra e da imagem;

V - o desenvolvimento econômico e tecnológico; e

VI - 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 envolvida em qualquer tratamento de dados a que se aplique esta Lei, independente de procuração ou de disposição contratual ou estatutária, deverá prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento desta Lei, 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 ao tratamento de dados pessoais cuja finalidade seja exclusivamente 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 e soberania nacional, segurança pública, repressão e investigação de infrações penais, atividades de inteligência, nos termos da Lei nº 9.883, de 7 de dezembro de 1999, e investigação destinada a apurar a prática de ato de improbidade, que serão regulados por legislação específica, observados os princípios gerais de proteção e os direitos previstos nesta lei;

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

III - anônimos ou anonimizados.

§ 6º O tratamento de dados pessoais previsto no inciso I, parágrafo 5º, deste artigo, será regido por legislação específica, observados os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

§ 7º É vedado o tratamento dos dados a que se refere o inciso I, do parágrafo 4º, deste artigo, por pessoa jurídica de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público.

§ 8º O dado pseudonimizado poderá ser compartilhado ou transferido a operador, sem a necessidade de consentimento do titular, observadas as condições estabelecidas no artigo 14, desta Lei, vedado o acesso ao ambiente controlado onde estejam armazenados os elementos identificadores.

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

I - anonimização: procedimento ou modificação destinada a impedir a associação de um dado pessoal a um indivíduo identificado ou identificável ou capaz de retirar do dado tratado informação, de maneira que o titular do dado não seja mais identificável;

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

VII - controlador: a pessoa natural ou a pessoa jurídica de direito público ou privado a quem competem as decisões referentes ao tratamento de dados pessoais e que determinam a finalidade e os meios para o tratamento de dados pessoais;

VIII - 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, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de sua coleta ou outra atividade de tratamento;

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

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

XI - dado pessoal sensível: qualquer dado pessoal que revele a convicção religiosa, política, sexual ou filosófica, a origem racial ou étnica, a participação em movimentos políticos ou sociais, informações médicas ou relacionadas a tratamento de saúde ou diagnósticos que revelem o estado de saúde físico ou mental do titular dos dados, dados referentes à vida sexual e suas informações genéticas ou biométricas;

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

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

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

XV – pessoa natural identificável: indivíduo que possa ser identificado, direta ou indiretamente, através de um elemento identificador, tais como nome, número de identificação, dados locacionais, identificadores eletrônicos;

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

XVII - 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.

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

I - licitude, boa-fé e finalidade determinada;

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 disponibilização ao titular de todas as informações relevantes 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;

XIII - 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 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 - 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, respeitado o segredo empresarial;

XII - tratamento não discriminatório de dados pessoais, assim compreendido aquele que violar direito e causar dano ao titular dos dados;

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 controlador 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 dez dias úteis, 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 controlador a sua retificação sem qualquer ônus.

§ 1º O controlador deverá, de forma gratuita, no prazo de até dez dias úteis, 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 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 controlador no prazo de até dez dias úteis.

Art. 9º Caso os pedidos a que se referem os artigos 6º a 8º, desta Lei, sejam manifestamente infundados ou excessivos, especialmente devido ao seu caráter recorrente, o controlador pode:

a) exigir o pagamento de um valor razoável, considerando os custos administrativos da retificação do dado pessoal, da comunicação ou da tomada das medidas solicitadas; ou

b) indeferir o pedido, informando ao titular dos dados, fundamentadamente, sua decisão.

Parágrafo único. Em qualquer caso previsto neste artigo, cabe ao controlador demonstrar, quando requisitado pela autoridade competente, o caráter manifestamente infundado ou excessivo dos pedidos.

Do Regime Jurídico do Tratamento de Dados Pessoais

Das Regras para Tratamento de Dados Pessoais

Art. 10. 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 ou regulatória pelo controlador;

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;

VII - quando necessário para atender aos interesses legítimos do controlador 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;

VIII - para o exercício regular de direitos em processo judicial, administrativo ou arbitral; ou

IX – pela administração pública, no atendimento de sua finalidade pública, visando à execução de competências legais e à formulação, implementação e avaliação de políticas públicas, inclusive por meio do compartilhamento de dados entre seus órgãos e entidades.

§ 1º O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I – quando o titular ou seu representante legal consentir de forma específica e expressa;

II – quando o tratamento for efetuado, no âmbito de atividades legítimas e com garantias adequadas, por fundação, associação ou qualquer outra entidade sem fins lucrativos de caráter político, filosófico, religioso ou sindical relacionado aos seus respectivos membros ou às pessoas que com ele mantenham contato periódico relacionado às suas finalidades, sendo vedado o seu acesso por terceiros sem o consentimento do titular, nos termos do inciso I, deste parágrafo 1º; ou

III - nas hipóteses previstas nos incisos III, IV, V, VIII e IX, do *caput*, deste artigo.

§ 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. 11. O legítimo interesse do controlador e de terceiro somente poderá fundamentar um tratamento de dados pessoais para a realização de finalidade legítima se não afetar de forma concreta os direitos e liberdades fundamentais do titular.

§ 1º O tratamento de dados pessoais fundamentado no legítimo interesse do controlador deve ser baseado em situações concretas em que a operação de tratamento seja necessária, que incluem, mas não se limitam a;

I – investigação, detecção e prevenção de irregularidades, fraudes e crimes;

II - transmissão de dados pessoais no âmbito de empresas de um mesmo grupo econômico para fins administrativos internos;

III- desenvolvimento e aprimoramento de produtos; ou

IV - inteligência corporativa.

§ 2º O controlador deverá oferecer mecanismos para que o titular se oponha ao tratamento realizado com base no legítimo interesse, cabendo ao primeiro demonstrar que seu legítimo interesse se sobrepõe à vontade do titular.

§ 3º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados, sendo recomendado o uso de técnicas de pseudonimização sempre que possível.

§ 4º A autoridade competente poderá solicitar, a qualquer tempo, ao controlador informações sobre tratamento que tiver o legítimo interesse como fundamento, incluindo relatório de impacto sobre a privacidade, preservado o sigilo empresarial.

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

Parágrafo único. 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.

Art. 13. O titular deve ter acesso a todas as informações relevantes acerca do tratamento dos seus dados, como finalidade, duração, identificação do controlador 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 Deverá ser informada ao titular qualquer alteração relativa à finalidade, à duração, ao controlador ou a outro elemento relevante do tratamento de dados, resguardado o disposto no parágrafo 2º, deste artigo.

§ 4º Aplica-se ao disposto neste artigo o parágrafo 3º, do artigo 6º, desta Lei.

Art. 14. O tratamento de dados para um fim diverso daquele para o qual os dados pessoais foram coletados somente pode ser realizado, nas hipóteses de tratamento que independem do consentimento do titular, se houver compatibilidade com a finalidade para a qual os dados foram coletados, observados, ainda:

I – o contexto da relação entre o controlador e o titular dos dados;

II – a natureza dos dados pessoais, especialmente quando se tratar de dados pessoais sensíveis;

III – as consequências do tratamento para o titular dos dados; e

IV – a adoção de medidas de segurança, tais como a criptografia e a pseudonimização.

Art. 15. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado no seu melhor interesse, observadas as seguintes disposições:

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

§ 2º O controlador e o operador deverão dar ampla publicidade à informação sobre os tipos de dados coletados e como são utilizados.

§ 3º O operador deve realizar todos os esforços razoáveis para verificar se o consentimento, foi dado pelos pais ou responsável legal pela criança, levando em consideração as tecnologias disponíveis.

§ 4º Os dados pessoais de crianças somente poderão ser coletados sem o consentimento dos pais ou do responsável legal quando o tratamento for necessário para assegurar sua proteção e socorro, não podendo ser comunicado a terceiros sem o consentimento a que se refere o § 1º, deste artigo.

§ 5º Somente os dados pessoais de crianças e adolescentes estritamente necessários poderão ser coletados, observada sua finalidade específica.

Art. 16. 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 e a possibilidade de guarda de informações mínimas necessárias ao combate a ilícitos ou fraudes; 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 histórica ou científica, excetuadas as atividades ou hipóteses previstas no artigo 2º, desta Lei; ou

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

Art. 17. A comunicação e a interconexão de dados pessoais sujeitam todos aqueles que tiverem acesso aos dados às mesmas obrigações legais e regulamentares do controlador.

Parágrafo único. Os critérios adicionais para a comunicação e a interconexão de dados pessoais serão definidos em regulamento.

Do tratamento de dados pessoais pelo poder público

Art. 18. O tratamento de dados pessoais pelas pessoas jurídicas de direito público 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 As disposições contidas nos incisos III e V, do artigo 4º, e no inciso V, do artigo 5º, são regidas, para o Poder Público, pela Lei nº 12.527, de 18 de novembro de 2011.

§ 3º Dados pessoais mantidos pela Administração Pública não são passíveis de cancelamento ou de oposição ao tratamento a pedido do titular, sendo respeitado o direito à retificação de dados incorretos, nos termos do art. 7º desta Lei.

§ 4º É permitida a comunicação ou a interconexão de dados pessoais entre órgãos e entidades públicas, respeitadas a finalidades previstas no *caput*, deste artigo, na forma do regulamento.

§ 5º 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. 19. 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 Cabe aos serviços de informações ao cidadão dos órgãos e entidades do Poder Público prestar informações adicionais sobre o tratamento, quando solicitados por interessados, nos termos da Lei nº 12.527, de 18 de novembro de 2011.

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

Art. 20. 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. 21. 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. 22. Os serviços notariais e de registro, exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas de direito público, nos termos desta Lei.

Art. 23. 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 2011; ou

II - Quando houver previsão legal.

§ 1º Nos casos previstos no inciso II, do *caput*, a transferência de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informada à autoridade competente e dependerá de consentimento do titular, exceto nas hipóteses de dispensa do consentimento previstas nesta lei.

Art. 24. A comunicação de dados pessoais entre órgãos e entidades de direito público será objeto de publicidade, na forma do regulamento.

Art. 25. A autoridade 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. 26. A autoridade competente poderá estabelecer normas complementares para as atividades de tratamento de dados pessoais por órgãos e entidades de direito público.

Art. 27. Quando houver infração a esta lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade competente poderá indicar medidas cabíveis para fazer cessar a violação.

Parágrafo único. As punições cabíveis a agente público no âmbito desta lei serão aplicadas na forma do previsto na Lei nº 12.527, de 18 de novembro de 2011.

Art. 28. A autoridade competente poderá solicitar a agentes do poder público a publicação de relatório 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. 29. O controlador, 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 às possibilidades de tratamento previstas no art. 10; 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 controlador e o operador devem manter, por cinco anos, registro das operações de tratamento de dados pessoais que realizarem, observada a regulamentação da autoridade competente.

§ 3º O prazo previsto no § 2º, deste artigo, poderá ser alterado pela autoridade competente em situações específicas, de acordo com a finalidade e as características do tratamento e a natureza do dado pessoal.

Art. 30. O controlador 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. 31. 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 controlador 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. 32. A transferência internacional de dados pessoais pode ser realizada nas seguintes hipóteses:

I - para países ou organismos internacionais que proporcionem nível adequado de proteção de dados, de acordo com critérios definidos em lei;

II - quando o titular, após ser devidamente informado do caráter internacional do tratamento, consentir de forma específica e destacada;

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

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

IV - quando a autoridade competente autorizar a transferência;

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

VI - quando a transferência for necessária para execução de política pública ou atribuição legal do serviço público, assegurada sua publicidade, nos termos desta Lei; ou

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

a) cláusulas contratuais específicas para determinada transferência;

b) cláusulas contratuais padrão ou normas corporativas globais dos responsáveis pelo tratamento de dados que fizerem parte de um mesmo grupo econômico; ou

c) certificações, selos ou instrumentos equivalentes emitidos por organismos de certificação reconhecidos ou credenciados pela autoridade competente.

§ 1º Os compromissos assumidos ao abrigo do disposto no inciso VII, do *caput*, deste artigo, vinculam o controlador, podendo a autoridade dispor sobre requisitos e condições mínimas a serem observados e verificar, a qualquer tempo, o cumprimento de tais requisitos.

§ 2º Para os fins do disposto no inciso I, do *caput*, deste artigo, as 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 o controlador, no âmbito de suas atividades, poderão requerer à autoridade competente a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.

Art. 33. O nível de proteção de dados de país estrangeiro ou de organismo internacional, nos termos do inciso I, do artigo 33, para fins de transferência internacional de dados, será avaliado pela autoridade competente, que deverá observar:

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

II – a natureza dos dados pessoais;

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, nos termos do regulamento;

V – a existência de garantias judiciais e institucionais que respeitem os direitos de proteção de dados pessoais; e

VI - outras circunstâncias específicas previstas em regulamento.

Art. 34. O controle do conteúdo de cláusula contratual padrão, de cláusula contratual específica para uma determinada transferência, de normas corporativas globais ou selos e certificados de conduta será realizado pela autoridade competente.

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

§ 2º Na análise de cláusula contratual, de documento ou de normas corporativas globais submetidas à aprovação da autoridade competente, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento.

§ 3º A autoridade competente poderá atestar organismos de certificação para a realização do previsto no *caput* deste artigo, sob sua fiscalização, nos termos definidos em regulamento;

§ 4º Os atos realizados por organismos de certificação poderão ser revistos pela autoridade competente e, caso em desconformidade com a presente lei, serão submetidos à observação de condições ou anulados.

§ 5º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no *caput* serão analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto no artigo 33.

Art. 35. Qualquer alteração nas garantias a que se refere o inciso VII, do artigo 32, deverão ser informadas à autoridade competente.

SEÇÃO V

Da Responsabilidade

Art. 36. O controlador ou o operador que, em razão do tratamento de dados pessoais, causar dano patrimonial, moral, individual ou coletivo, em violação ao disposto nesta Lei, 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 previstas nesta Lei ou as instruções lícitas do controlador, hipótese em que o operador equipara-se a controlador, salvo as hipóteses de exclusão do artigo 37.

II - respondem solidariamente os controladores que estiverem conjuntamente envolvidos em tratamento do qual decorreu dano ao titular dos dados, salvo as hipóteses de exclusão do artigo 37.

§ 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 ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

§ 3º A defesa dos interesses e direitos dos titulares dos dados pessoais poderá ser exercida em juízo individualmente ou a título coletivo, observado, no que couber, o disposto no Título III, da Lei nº 8.078, de 11 de setembro de 1990.

§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua culpabilidade.

Art. 37. Aqueles que tiverem acesso aos dados pessoais só não serão responsabilizados, nos termos desta Seção, quando provarem:

I - que não realizaram o tratamento de dados pessoais que lhes foi atribuído;

II - que, embora tenham realizado o tratamento de dados pessoais que lhes foi 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. 38. O tratamento de dados pessoais será irregular, quando deixar de observar as disposições desta Lei e quando não fornecer a segurança que o titular dele pode esperar, levando-se em consideração 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 controlador ou o operador que, ao deixar de adotar as medidas de segurança previstos nesta Lei, der causa à violação.

SEÇÃO VI

Da Governança em Privacidade

Art. 39. Na aplicação dos princípios indicados nos incisos IX e X, do art. 4º, desta lei, o controlador deverá:

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

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

b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo 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. 40. A União fiscalizará o cumprimento desta lei, apenando eventuais infrações mediante processo administrativo que assegure o contraditório e a ampla defesa.

Art. 41. A autoridade competente designada para zelar pela implementação e pela fiscalização desta Lei 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;

XI – implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações individuais ou coletivas sobre tratamento de dados pessoais em desconformidade com esta Lei;

XII - estabelecer medidas adicionais de segurança e de proteção aos dados pessoais sensíveis, que deverão ser adotadas pelo controlador e por outros agentes do tratamento, bem como solicitar a apresentação de relatório de impacto à privacidade; e

XI - editar normas complementares para a proteção de dados pessoais, inclusive quanto aos elementos e às informações mínimas que deverão constar do relatório de impacto a que se refere esta Lei.

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. 42. 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 ou bloqueio;

III - cancelamento dos dados;

IV - multa de até 2% sobre o faturamento da empresa ou do grupo econômico no Brasil no seu último exercício, excluídos os tributos;

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

VI - 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 artigo 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 e somente poderão dispor sobre as penalidades referidas nos incisos II e V, deste artigo.

§ 3º A autoridade competente poderá notificar o controlador, 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.

§ 5º Determinada pela autoridade competente a aplicação de sanção de pagamento de multa ou de obrigação de fazer ou não fazer, o representante legal constituído no Brasil da empresa sediada no exterior deverá ser notificado e intimado.

Art. 43. 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. 30 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. 44. 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. 45. O pagamento da multa ou o cumprimento da obrigação de fazer ou não fazer de empresa controladora sediada no exterior pode ser exigido da filial, agência, sucursal, estabelecimento ou escritório instalado no Brasil.

Art. 46. 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. 47. 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. 48. 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. 49. Ficam revogadas as disposições em contrário, inclusive os incisos VII, VIII e IX, do artigo 7º, da Lei nº 12.965, de 23 de abril de 2014.

Parágrafo único. A Lei nº 12.965, de 23 de abril de 2014, passa 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 previstas em lei;"(NR)
>
> "Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda, ressalvado o disposto em lei de proteção de dados:
>
> ....."(NR)

Art. 50. A autoridade competente estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, com relação ao tratamento desses dados realizado sob a vigência desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados.

Art. 51. As atividades, atribuições e competências estabelecidas à autoridade competente a que se refere esta lei serão exercidas por órgão definido em decreto, em caráter transitório, até que o Poder Executivo venha a constituir entidade destinada a essa finalidade.

Art. 52. Os prazos a que se referem o parágrafo 1º, do artigo 6º, o parágrafo 1º, do artigo 7º, e o *caput* do artigo 8º serão de trinta dias no primeiro ano de vigência desta Lei.

Art. 53. Esta lei entra em vigor após decorrido trezentos e sessenta e cinco dias de sua publicação oficial.

Sala das Sessões,

, Presidente

, Relator