

## PROJETO DE LEI Nº 5.276/2016

(Do Poder Executivo)

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

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

2. É louvável a iniciativa e merece aprovação pelo Poder Legislativo, colocando o Brasil no rol dos países que protegem a privacidade de seus cidadãos. Embora já tenha havido diversos avanços no texto proposto desde a sua apresentação, ainda há algumas reformas relevantes e necessárias para assegurar-se o efeito que se pretende obter para os titulares sem a disruptura do modelo econômico nacional, capaz de alijar o Brasil da economia e do desenvolvimento globais.

### **3. DA RELEVÂNCIA DOS ORGÃOS DE PROTEÇÃO AO CRÉDITO**

Antes de passar à análise do projeto, devemos examinar o reflexo que tal proposição terá sobre a atividade exercida pelos órgãos de proteção ao crédito e conseqüentemente, para a economia e a sociedade brasileira.

Nesse sentido, deve-se considerar o atual “modus operandi” da sociedade de consumo e as condições a serem observadas pelos órgãos de proteção ao crédito para a anotação de informações sobre consumidores, no âmbito de sua atividade hoje já regulada pelo art. 43 da Lei nº 8.078/90 - Código de Defesa do Consumidor, pela Lei nº 9.507/97 - Lei do *Habeas Data*, pela Lei nº 12.414/2011 – Cadastro Positivo e sua regulamentação posterior (Decreto nº 7.829/2012 e resoluções do CMN).

Os bancos de dados dos serviços de proteção ao crédito registram apenas informações necessária e pertinentes para a tomada de decisão de concessão de crédito ou realização de negócios, não armazenando, para tanto, quaisquer informações sensíveis ou confidenciais, que possam afetar a intimidade ou a privacidade dos indivíduos. Visam, apenas, a permitir que os seus clientes concedam crédito ou realizem negócios com a necessária segurança acerca do recebimento da contrapartida esperada, propiciando a adoção de medidas preventivas ao superendividamento e ao inadimplemento do consumidor na disponibilização de crédito. Tal é a relevância das atividades exercidas pelos bancos de dados de proteção ao crédito – cujas informações são um dos pilares das políticas de concessão de recursos e aplicação de juros – que estes possuem caráter público<sup>1</sup>.

Essas especificidades, haja vista a sua relevância, devem ser adequadamente tratadas pelo legislador ao endereçar normas de aplicação geral, de modo a não onerar a ponto de inviabilizar setores específicos que são cruciais para a economia do País, como os bancos de dados de proteção ao crédito. Por esse motivo, passamos a discorrer sobre os aspectos cujo alinhamento consideramos essenciais para o setor.

---

<sup>1</sup> Código de Defesa do Consumidor: Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. (...)

§ 4º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.

#### **4. MODIFICAÇÕES AO PROJETO.**

A seguir, serão tecidos os argumentos técnicos e jurídicos que pautam as modificações abaixo:

##### **CAPÍTULO I**

##### **DISPOSIÇÕES PRELIMINARES**

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

Art. 2º A disciplina da proteção de dados pessoais tem como fundamento o respeito à privacidade e:

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

- I - a operação de tratamento seja realizada no território nacional;
- II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
- III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

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

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

- I - realizado por pessoa natural para fins exclusivamente pessoais;
- II - realizado para fins exclusivamente jornalísticos, artísticos, literários ou acadêmicos; ou
- III - realizado para fins exclusivos de segurança pública, de defesa nacional, de segurança do Estado ou de atividades de investigação e repressão de infrações penais.

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

§ 2º É vedado o tratamento dos dados a que se refere o inciso III por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico ao órgão competente.

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

**Inclusão do inciso IV** – *“disponíveis ao público ou de conhecimento geral por iniciativa ou com a prévia ciência do titular.”*

**Justificativa:** As informações que já são de domínio público não devem estar no escopo da regulamentação aqui tratada por estarem disponíveis a qualquer interessado, quer porque essa disponibilização fazia parte do escopo dos serviços conforme informação clara a ser-lhe fornecida no ato da adesão, quer porque o usuário promoveu a publicação ou disponibilização da informação ou por qualquer outro motivo licitamente válido.

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

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

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

III - dados sensíveis: dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos;

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

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

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

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

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

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

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

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

XII - anonimização: qualquer procedimento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

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

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

XV - uso compartilhado de dados: a comunicação, a difusão, a transferência internacional, a interconexão de dados pessoais ou o tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos, no cumprimento de suas competências legais, ou entre órgãos e entidades públicos e entes privados, com autorização específica, para uma ou mais modalidades de tratamento delegados por esses entes públicos.

**Modificação do inciso I** - inclusão do termo “pelo responsável pelo tratamento de dados pessoais”, passando o inciso I a constar com a seguinte redação - “*dado pessoal: dado relacionado à pessoa natural identificada ou razoavelmente identificável pelo responsável pelo tratamento de dados pessoais, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa;*”

**Justificativa:** de acordo com o artigo 1º desta Lei, a sua finalidade é “proteger os direitos fundamentais de liberdade, intimidade e privacidade da pessoa natural” (grifamos). Logo, para que haja potencial prejuízo a tais direitos, é preciso que seja possível determinar a pessoa natural a quem um conjunto de dados se refere.

Ocorre que, atualmente, muitos dados que, nos termos da definição contida no inciso em análise, estariam classificados como pessoais, são captados de forma completamente anônima, de modo que seria necessário um grande custo e tempo para determinar a identidade do indivíduo, ainda com determinado grau de imprecisão na análise. Por conseguinte, embora seja tecnicamente possível, é altamente improvável que a identificação dos dados seja feita porque, para o fim para o qual foram coletados, é desnecessária.

Por isso, sugerimos o ajuste do conceito originalmente proposto, a fim de excepcionar os dados pessoais que não sejam razoavelmente identificáveis. Vale destacar que entendemos ser inviável detalhar as tecnologias compreendidas como razoáveis haja vista a constante atualização das ferramentas atualmente existentes.

Especificamente sobre os dados locacionais e identificadores eletrônicos, é importante considerar que não necessariamente identificam uma pessoa natural, razão pela qual sugerimos que o conceito de dado pessoal aqui constante seja aplicado apenas aos casos em que a atribuição a uma pessoa natural seja, de fato, inequívoca.

Veja-se, por exemplo, que um endereço de IP (Protocolo de Internet) é um dado mutável que identifica um equipamento, e não uma pessoa (art. 5º, inc. III, da Lei nº 12.965/2014). Pode, aliás, ser utilizado por diversas pessoas, não sendo possível individualizá-las com total segurança jurídica.

**Modificação do inciso III:** exclusão do termo “biométricos” no inciso III, passando a contar com a seguinte redação – “*dados sensíveis: dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual e dados genéticos*”;

**Justificativa:** O avanço tecnológico implica o uso dos dados biométricos especificamente para a identificação dos indivíduos. Logo, estes dados, embora mereçam proteção, não podem ser considerados sensíveis, mesmo porque a principal característica dos dados sensíveis é identificar tudo aquilo que tenha a ver com a intimidade da pessoa, e não com a sua identificação em sociedade.

**Modificação do inciso IV:** *“dados anonimizados: dados relativos a um titular que não seja identificado pelo responsável para a finalidade a que se destina o tratamento. A eventual desanonimização, por qualquer pessoa, sujeita-a ao cumprimento desta Lei;”*

**Justificativa:** há diversas situações em que não é necessária a identificação do titular para o tratamento de seus dados pessoais, como, por exemplo, para estudos e desenvolvimentos a fim de apurar a relevância de determinados grupos de informações. Portanto, ainda que seja possível identificar o titular, o responsável pode optar por não fazê-lo, armazenando e tratando os dados de forma anônima.

Devido à evolução tecnológica, a existência de meios suscetíveis a identificar o titular dos dados anônimos será, a cada dia, mais frequente e acessível. Porém, se o responsável pelo tratamento não fizer uso dessas tecnologias, os dados não deixarão de ser anônimos pela simples existência de tais mecanismos de desanonimização e, conseqüentemente, não haverá qualquer prejuízo à liberdade, privacidade ou intimidade de seus titulares.

Logo, o que se deve cuidar é para que, em caso de desanonimização, apliquem-se as disposições desta lei de modo a proteger a liberdade, a privacidade e a intimidade dos titulares, tratando-se adequadamente a exceção à regra com a aplicação desta lei caso ocorra a desanonimização.

**Inclusão do inciso V,** renumerando-se os subseqüentes - *“dados cadastrais: dado pessoal que identifica o titular, mas que não representa comportamento ou relação de convivência privada, assim consideradas as informações sobre a filiação, os endereços físico e eletrônico, o documento de identificação oficial do usuário e a qualificação pessoal, entendida como nome, prenome, data de nascimento, estado civil e profissão do usuário.”*

**Justificativa:** inicialmente, cumpre destacar que não se propõe, aqui, excluir os dados cadastrais do conceito de dados pessoais, pois indubitavelmente o integram. Propõe-se, apenas, a harmonização dos interesses público e privado no tratamento de tais informações, razão pela qual se faz necessário definir a espécie separadamente do gênero, a exemplo do que se fez em relação aos dados sensíveis.

É certo que os dados cadastrais não revelam quaisquer aspectos relativos à vida privada ou à intimidade do indivíduo. São, ao contrário, informações objetivas e não sensíveis, alguns até provenientes de órgãos públicos, utilizadas tão somente como elementos que tornam possível a correta e segura identificação, bem como a comunicação entre os indivíduos inseridos dentro de uma sociedade. Além disso, sendo objetivos esses dados, não permitem qualquer juízo de valor sobre a pessoa. O endereço eletrônico (e-mail) é ainda menos privativo do que o endereço físico, identificando apenas onde as correspondências de um usuário podem ser entregues, sem demonstrar sequer a sua localização. Serve, apenas, para viabilizar a comunicação rápida e efetiva com o seu titular.

Logo, é necessária a harmonização da proteção aos dados cadastrais com o interesse público prevalecente em identificar adequadamente as pessoas em sociedade e a agilidade da comunicação, a fim de evitar que a pretensa proteção à privacidade, nos casos em que não há, de fato, interesse a ser protegido, possa inviabilizar atividades hoje essenciais à vida em sociedade. Os dados pessoais que identificam os indivíduos de forma simples e objetiva e que, normalmente, circulam livremente em sociedade, como nome, data de nascimento, registros de identificação civil e fiscal, telefone e endereço, não merecem sujeitar-se à regra do consentimento.

Nesse sentido, é a tese do Professor Tércio Sampaio Ferraz Junior, em seu trabalho “Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado”, publicado na Revista da Faculdade de Direito; vol. 88; 1993; pp. 449/50, ao tratar dos dados não sigilosos, indispensáveis à correta e à segura identificação dos indivíduos: **“Pelo sentido inexoravelmente comunicacional da convivência, a vida**

**privada compõe, porém, um conjunto de situações que, usualmente, são informadas sem constrangimento. São dados que, embora privativos** - como o nome, endereço, profissão, idade, estado civil, filiação, número de registro público oficial etc., **condicionam o próprio intercâmbio humano em sociedade**, pois constituem elementos de identificação que tornam a comunicação possível, corrente e segura. Por isso, a proteção desses dados em si, pelo sigilo, não faz sentido. Assim, a inviolabilidade de dados referentes à vida privada só tem pertinência para aqueles associados aos elementos identificadores usados nas relações de convivência, as quais só dizem respeito aos que convivem. Dito de outro modo, **os elementos de identificação só são protegidos quando compõem relações de convivência privadas: a proteção é para elas, não para eles. Em consequência, simples cadastros de elementos identificadores (nome, endereço, R.G., filiação, etc.) não são protegidos.** Mas cadastros que envolvam relações de convivência privada (por exemplo, nas relações de clientela, desde quando é cliente, se a relação foi interrompida, as razões pelas quais isto ocorreu, quais os interesses peculiares do cliente, sua capacidade de satisfazer aqueles interesses, etc.) estão sob proteção. Afinal, o risco à integridade moral do sujeito, objeto do direito à privacidade, não está no nome, mas na exploração do nome, não está nos elementos de identificação que condicionam as relações privadas, mas na apropriação dessas relações por terceiros a quem elas não dizem respeito” (destaques nossos).

Sendo o escopo da lei, expresso em seu artigo 1º, proteger a intimidade e a vida privada das pessoas naturais, é razoável dispensar o consentimento para o tratamento dos dados que não tenham o potencial de afetar tais direitos fundamentais, como as informações de identificação que visam tão somente a individualizar uma pessoa em sociedade, bem como proteger a coletividade e os próprios indivíduos, como, por exemplo, na prevenção contra fraudes. **Este conceito de dados cadastrais, inclusive, já foi parcialmente acolhido no Decreto nº 8.771/2016, que regulamentou a Lei nº 12.965/2014 (Marco Civil da Internet).**

Tal exceção, contudo, não exime os responsáveis pelo tratamento do dever de assegurar o acesso dos titulares às suas informações e retificá-las, na forma desta lei.

**Inclusão dos incisos reenumerados como VII e VIII**, reenumerando-se os subsequentes, com a seguinte redação:

*“VII – fonte: pessoa natural ou jurídica que fornece informações para os bancos de dados;*

*VIII – consulente: pessoa natural ou jurídica que consulta informações disponíveis nos bancos de dados”;*

**Justificativa:** em que pese ser importante definir o responsável pelas decisões referentes ao tratamento dos dados pessoais, é importante considerar que este pode ser gestor do banco de dados, a fonte ou o consulente, motivo pelo qual é recomendável que tais conceitos também sejam incluídos na norma para a adequada identificação de responsáveis e atribuição de responsabilidades, conforme será sugerido adiante.

**Modificação do atual inciso IX**, substituindo-se o termo “operador” por “gestor do banco de dados”:  
*“gestor de banco de dados: a pessoa jurídica, de direito público ou privado, contratada pelo responsável pelo banco de dados, encarregada do tratamento de dados pessoais sob as orientações daquele.”*

**Justificativa:** nos termos da justificativa anterior, trata-se de adequação da nomenclatura àquela já empregada em diploma legal vigente (Lei do Cadastro Positivo).

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

I - finalidade: pelo qual o tratamento deve ser realizado para finalidades legítimas, específicas, explícitas e informadas ao titular, não podendo ser tratados posteriormente de forma incompatível com essas finalidades;

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

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

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

**Comentário:** a consulta facilitada aos dados é um mecanismo de controle importante para que os titulares dos dados pessoais possam avaliar a veracidade e atualização dos registros a eles correspondentes, assegurando a sua precisão. Essa facilitação, contudo, deve ser interpretada de modo a preservar a segurança das informações e a adequada verificação da identidade do solicitante, cumprindo, assim, a proteção de sua intimidade e privacidade.

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

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

VII - segurança: pelo qual devem ser utilizadas medidas técnicas e administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: pelo qual devem ser adotadas medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; e

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

**Modificação do inciso I:** *“finalidade: pelo qual o tratamento deve ser realizado para finalidades legítimas e devidamente informadas ao titular;”*

**Justificativa:** a finalidade do tratamento deve corresponder àquela informada ao titular no momento da coleta dos dados pessoais. Há necessidade de exclusão das palavras “específicas” e “explícitas”, visto que, em muitos casos, a finalidade está descrita em termos de uso ou políticas de privacidade do responsável ou por outros meios que resultam em grandes volumes diários, o que torna incompatível a redação proposta.

No entanto, o titular deve ser devidamente informado no momento da coleta de seus dados, de forma clara e transparente sobre o tratamento a ser realizado, e caso seja realizado em desconformidade com o que foi consentido, poderá revogar o consentimento a qualquer momento, sem prejuízo da apuração da responsabilidade do responsável pelo tratamento.

**Modificação do inciso II**, substituindo-se a expressão “legítimas expectativas do titular” por “informadas ao titular”, haja vista a subjetividade do conceito atual: *“adequação: pelo qual o tratamento deve ser compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento;”*

**Justificativa:** adequação é, a rigor, a correspondência entre o que é proposto e o que é efetivamente realizado. Logo, a “legítima expectativa do titular” deve corresponder aos fins que lhe foram informados e para os quais consentiu com o tratamento de seus dados pessoais. Por esse motivo, sugere-se que o conceito ora subjetivo, traduzido pela expectativa do titular, seja substituído pela análise objetiva da correspondência entre a finalidade informada ao titular e aquela efetivamente dada às informações.

**Modificação do inciso V**: *“qualidade dos dados: pelo qual devem ser garantidas aos titulares a integridade dos dados fornecidos pelas fontes para o cumprimento da finalidade de seu tratamento;”*

**Justificativa:** a exatidão e a atualização dos dados competem às fontes que os informarem para tratamento, haja vista que somente a elas cabe conhecer e controlar as transações ou os fatos que os originaram. Portanto, as fontes são responsáveis pela obtenção e fornecimento dos dados e, por consequência, as empresas que realizam o seu tratamento devem ser responsáveis por manter a integridade dessas informações tais como recebidas. Para que as fontes possam proceder à retificação ou à atualização dos apontamentos, cabe aos gestores de bancos de dados prover os meios necessários para o recebimento das respectivas solicitações.

Trata-se, portanto, de adequação para que não acarrete insegurança jurídica acerca da responsabilidade das empresas que tratam os dados coletados por terceiros.

Ressalte-se, ainda, que, em muitos casos, a obrigação pela atualização das informações é do próprio titular dos dados, citando-se, como exemplo, a obrigação do devedor de informar ao credor a eventual alteração em seus dados.

**Modificação do inciso VI**, com vistas a ressaltar a proteção ao segredo empresarial: *“transparência: pelo qual devem ser garantidas aos titulares informações claras, adequadas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, resguardado o segredo empresarial;”*

**Justificativa:** cabe ao titular o direito de acessar e conhecer todas as informações captadas a seu respeito para, querendo, retificá-las ou atualizá-las. Deve, ainda, conhecer a finalidade do seu tratamento e, em linhas gerais, como este será realizado. Por outro lado, deve-se observar o segredo empresarial que assegura, em diversos casos, a viabilidade da existência do tratamento em si, como, por exemplo, nos casos dos modelos de probabilidade de pagamento, que constituem em si um serviço cuja fórmula diferencia os diversos prestadores no mercado.

**Modificação do inciso IX**, para que se inclua o termo “não justificáveis” após a palavra “discriminatórios”: *“não discriminação: pelo qual o tratamento não pode ser realizado para fins discriminatórios não justificáveis.”*

**Justificativa:** é importante que se tenha em conta que a discriminação não é coibida pelo Direito. Ao contrário, ela é necessária para a correta aplicação do princípio constitucional da isonomia, tratando-se igualmente os iguais e desigualmente os desiguais, na medida de sua desigualdade. O que se deve coibir, em verdade, é a discriminação injustificada. Logo, sugere-se a adequação acima.

## REQUISITOS PARA O TRATAMENTO DE DADOS PESSOAIS

### Seção I

#### Requisitos para o tratamento

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

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

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

III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis ou regulamentos;

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

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

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

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

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

IX - quando necessário para atender aos interesses legítimos do responsável ou de terceiro, exceto no caso de prevalecerem interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for menor de idade.

§ 1º Nos casos de aplicação do disposto nos incisos II e III, o responsável deverá informar ao titular as hipóteses em que será admitido o tratamento de seus dados.

§ 2º A forma de disponibilização das informações previstas no parágrafo anterior e no art. 24 poderá ser especificada pelo órgão competente.

§ 3º No caso de descumprimento do disposto no § 1º, o operador ou o responsável pelo tratamento de dados poderá ser responsabilizado.

§ 4º O tratamento de dados pessoais cujo acesso é público deve ser realizado de acordo com esta Lei, considerados a finalidade, a boa-fé e o interesse público que justificaram a sua disponibilização.

**Modificação do inciso V**, para que possa abranger o tratamento de dados pessoais por terceiros alheios à relação contratual mas que são necessários para suportá-la: *“quando necessário para a execução de um contrato ou de procedimentos preliminares relacionados a um contrato do qual é parte o titular;”*

**Justificativa:** previamente à formalização de um contrato, as partes precisam analisar a viabilidade e as condições aplicáveis à realização do negócio. O tratamento dos dados para decisões de crédito realizado por terceiro que consolida todas as informações disponíveis para tanto (banco de dados de proteção ao crédito) é fundamental para a realização de negócios entre as partes, mesmo que, em análise prévia,

ainda não exista a manifestação de vontade de uma delas. Cite-se, como exemplo, os créditos pré-aprovados para agilizar o atendimento das demandas de consumidores. Para que isso seja possível, é importante que todas as informações relevantes para a análise de crédito já tenham sido coletadas, processadas e estejam disponíveis nas bases de dados no momento da consulta, munindo os credores de dados relevantes para apoiar decisões que propiciem medidas preventivas ao inadimplemento e ao superendividamento do consumidor na disponibilização de crédito. Vale lembrar, por fim, que é direito do credor avaliar o tomador ainda que não seja da vontade deste a referida análise, pois deve ser-lhe assegurado precaver-se contra eventual inadimplência.

**Modificação do inciso IX**, para que se especifiquem as situações em que se requer proteção diferenciada, nos seguintes termos: *“IX - quando necessário para atender aos interesses legítimos do responsável ou de terceiro, exceto no caso de se tratar de dados sensíveis ou quando o titular for menor de idade.”*

**Justificativa:** a redação originalmente proposta, no ambiente atípico de alta litigiosidade da sociedade brasileira, traz insegurança jurídica aos responsáveis pelo tratamento de dados ao não especificar os interesses ou liberdades fundamentais que prevalecem sobre o que o tratamento que o próprio inciso legitima. Veja-se que a proteção aos dados pessoais decorre *de per se* da garantia aos direitos fundamentais à intimidade e à vida privada. Por esta razão, sugere-se definir as situações em que o interesse legítimo não pode prevalecer sobre o consentimento do titular, nomeadamente, a nosso ver, quando se tratar de dados sensíveis ou de menor de idade, conforme ora sugerido.

**Inclusão dos incisos X, XI e XII**, nos seguintes termos: *“X – para anotar o inadimplemento de obrigações pelo titular mediante solicitação do credor a bancos de dados de proteção ao crédito, devendo o titular ser comunicado nos termos do art. 43 da Lei nº 8.078/90 – Código de Defesa do Consumidor; XI – para a formação, o processamento e a consulta a dados cadastrais; XII – para a prevenção a fraudes.”*

**Justificativa:** o consentimento, conforme decorre desta proposta, é uma forma de assegurar ao titular o efetivo controle sobre a circulação de seus dados pessoais, com objetivo de proteger a sua privacidade e intimidade, direitos fundamentais amparados pela Constituição Federal. É, portanto, relevante e necessária a sua coleta quando se tratar de dados que possuam, em si, potencial de prejudicar a privacidade e a intimidade dos indivíduos, sem que, com isso, haja prejuízo ao supremo interesse público e da coletividade. Por outro lado, quando presentes os pressupostos de (i) inexistência de potencial ofensivo à privacidade e intimidade e (ii) relevante interesse público, é admissível a dispensa do consentimento, conforme se verá.

Porém, antes de passar à justificativa de tais exceções, é importante que se considere, na edição de tão relevante diploma legal para os cidadãos brasileiros, a experiência internacional e os reflexos que os requisitos ora previstos podem ter não apenas para os titulares, mas para toda a sociedade e a economia. Cite-se, como exemplo do imprescindível cuidado na análise das consequências concretas e na busca do formato mais adequado para a efetiva proteção de todos os direitos individuais e coletivos envolvidos neste projeto de lei, a Lei do Cadastro Positivo, cujos requisitos para a sua formação terminaram por retardar e quiçá inviabilizar a sua efetiva implementação do país, deixando-o à margem das grandes economias mundiais no que tange ao potencial de incrementar o acesso da população ao crédito e controlar o superendividamento.

Para apoiar esta análise, anexamos a este documento um estudo realizado pelo conceituado instituto de pesquisa americano Policy and Economic Research Council - PERC, na versão original em inglês e a sua

tradução para o português, que apresenta um panorama geral sobre a legislação comparada em proteção de dados pessoais.

Especificamente no que se refere à **inclusão do inciso X**, busca-se evidenciar que a anotação de inadimplência independe de consentimento, embora deva ser comunicada ao titular na forma do art. 43 do Código de Defesa do Consumidor. Evita-se, assim, interpretações divergentes sobre a aplicabilidade do Código de Defesa do Consumidor e a sua prevalência sobre a Lei de Proteção de Dados Pessoais, bem como mitiga-se o risco de criar-se uma nova indústria de dano moral acerca do tema.

Veja-se que as informações negativas referem-se a obrigações não pagas pelos devedores e que podem influenciar na análise de crédito por futuros concedentes, razão pela qual a sua divulgação normalmente não interessa aos devedores, sobretudo se estiverem buscando uma nova contratação de crédito. Logo, pela própria natureza das informações negativas, seria um contrassenso condicionar a sua disponibilização aos legítimos interessados ao prévio consentimento do inadimplente, que certamente não o concederia.

De acordo com estudo realizado pela Serasa Experian, a exclusão das informações de inadimplência nos modelos de análise de risco de crédito, por exemplo, prejudicaria a sua eficiência e, com isso, a previsibilidade dos concedentes de crédito sobre os riscos assumidos em novas concessões.

Com base em modelo econométrico que relaciona o PIB com a concessão de crédito com recursos livres às pessoas físicas (ambas variáveis deflacionadas pela inflação oficial IPCA), estimamos uma elasticidade do PIB em relação ao crédito de 0,33, ou seja, para cada 1% de redução na concessão de crédito com recursos livres às pessoas físicas haveria uma retração de 0,33% no PIB. Portanto, teríamos uma retração de, aproximadamente, 26% no PIB (deflacionado), fazendo-o retroagir ao nível de 2007.

Sabendo-se que o próprio Banco Central do Brasil estima, em seu Relatório de Economia Bancária e Crédito – 2014, que a inadimplência chega a corresponder a cerca de 33% do spread bancário, seria inevitável o impacto no bolso do consumidor em termos de quão mais caro ele teria que pagar pelos financiamentos caso as condições de análise e concessão de crédito se deteriorassem em função da perda de performance dos modelos de análise de risco de crédito face à aplicação da lei, sem que disso resulte qualquer benefício para a sociedade.

O **inciso XI**, a seu turno, versa sobre os dados cadastrais, ou seja, os dados pessoais que identificam os indivíduos de forma simples e objetiva e que, normalmente, circulam livremente em sociedade, como nome, data de nascimento, nome da mãe, registros de identificação civil e fiscal, telefone e endereço. Haja vista a inexistência de potencial ofensivo à privacidade e à intimidade que decorre destes dados, estes não merecem sujeitar-se à regra do consentimento, o que é fundamental, por exemplo, para a prevenção a fraudes e pressupõe a preexistência de uma base de informações que possa ser consultada para análise.

Nesse sentido, é a tese do Professor Tércio Sampaio Ferraz Junior, em seu trabalho “Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado”, publicado na Revista da Faculdade de Direito; vol. 88; 1993; pp. 449/50, ao tratar dos dados não sigilosos, indispensáveis à correta e à segura identificação dos indivíduos: **“Pelo sentido inexoravelmente comunicacional da convivência, a vida privada compõe, porém, um conjunto de situações que, usualmente, são informadas sem constrangimento. São dados que, embora privativos - como o nome, endereço, profissão, idade, estado civil, filiação, número de registro público oficial etc., condicionam o próprio intercâmbio humano em sociedade, pois constituem elementos de identificação que tornam a comunicação possível, corrente e segura.** Por isso, **a proteção desses dados em si, pelo sigilo, não faz sentido.** Assim, a inviolabilidade de dados referentes à vida privada só tem pertinência para aqueles associados aos elementos identificadores

usados nas relações de convivência, as quais só dizem respeito aos que convivem. Dito de outro modo, **os elementos de identificação só são protegidos quando compõem relações de convivência privadas: a proteção é para elas, não para eles. Em consequência, simples cadastros de elementos identificadores (nome, endereço, R.G., filiação, etc.) não são protegidos.** Mas cadastros que envolvam relações de convivência privada (por exemplo, nas relações de clientela, desde quando é cliente, se a relação foi interrompida, as razões pelas quais isto ocorreu, quais os interesses peculiares do cliente, sua capacidade de satisfazer aqueles interesses, etc.) estão sob proteção. Afinal, o risco à integridade moral do sujeito, objeto do direito à privacidade, não está no nome, mas na exploração do nome, não está nos elementos de identificação que condicionam as relações privadas, mas na apropriação dessas relações por terceiros a quem elas não dizem respeito” (destaques nossos).

Sendo o escopo da lei, expresso em seu artigo 1º, proteger a intimidade e a vida privada das pessoas naturais, é razoável dispensar o consentimento para o tratamento dos dados que não tenham o potencial de afetar tais direitos fundamentais, como as informações de identificação que visam tão somente a individualizar uma pessoa em sociedade, bem como proteger a coletividade e os próprios indivíduos contra fraudes.

Por fim, no que se refere ao **inciso XII**, importa destacar que, segundo estudo da Serasa Experian, é possível estimar qual seria o impacto da lei sobre as fraudes por meio da perda de performance prevista para as soluções que visam a preveni-la e que utilizam a completude das informações identificadoras disponíveis nas bases de dados.

Estima-se que o impacto para o mercado, com base apenas nos serviços prestados pela Serasa Experian, seja de R\$ 479 milhões, considerando-se que (i) as soluções antifraude preveniram, entre os meses de julho/14 e junho/15, perdas que somaram R\$ 279 milhões; e (ii) para as soluções nas quais não temos o “feedback” real do cliente, embora saibamos que há aproximadamente 2 milhões de tentativas a fraude, considerou-se um ticket médio conservador de R\$ 100, representando, portanto, uma perda financeira adicional de cerca de R\$ 200 milhões.

Vale destacar que a dispensa do consentimento em nada deve prejudicar o direito dos titulares de conhecer e acessar, a qualquer tempo, as informações identificadoras registradas a seu respeito e requerer a sua retificação, se o caso.

Busca-se, assim, preservar, de forma equilibrada, a proteção dos titulares, a sua liberdade de escolha, o livre exercício empresarial dos responsáveis pelo tratamento e o desenvolvimento econômico e social do país.

**Modificação do § 3º do art. 7º**, substituindo-se o termo “operador” por “gestor de banco de dados”, nos seguintes termos: *“No caso de descumprimento do disposto no § 1º, o gestor de banco de dados ou o responsável pelo tratamento de dados poderá ser responsabilizado”.*

**Justificativa:** conforme justificativa apresentada no artigo 5º, trata-se de adequação da nomenclatura àquela já empregada em diploma legal vigente (Lei do Cadastro Positivo).

**Modificação do § 4º do art. 7º**, para que se diferenciem os dados públicos dos privados, passando a constar da seguinte forma: *“O tratamento de dados pessoais cujo acesso é público deve ser realizado de acordo com a finalidade, a boa-fé e o interesse público que justificaram a sua disponibilização.”*

**Justificativa:** segundo o art. 5º, inc. XXXIII, da Constituição Federal, “todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão

prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado”.

A Lei de Acesso a Informação (Lei nº 12.527/2011), ao regulamentar o direito fundamental à informação, estabeleceu as seguintes diretrizes:

- “I - observância da publicidade como preceito geral e do sigilo como exceção;
- II - divulgação de informações de interesse público, independentemente de solicitações;
- III - utilização de meios de comunicação viabilizados pela tecnologia da informação;
- IV - fomento ao desenvolvimento da cultura de transparência na administração pública;
- V - desenvolvimento do controle social da administração pública”.

Cabe, portanto, aos órgãos integrantes da Administração Pública assegurar o acesso aos dados públicos a todos que lhe solicitarem, inclusive divulgando-os independentemente de solicitação, resguardando-se, por óbvio, os dados cujo sigilo é imprescindível para a segurança da sociedade e do Estado.

Destaca-se a decisão do Superior Tribunal de Justiça que, em julgamento dos Recursos Especiais avocados como Repetitivos nºs 1444469-DF e 1344352-SP, decidiu pela desnecessidade de comunicar-se aos consumidores a inclusão de informações provenientes de fonte pública em bancos de dados de proteção ao crédito.

Vale destacar a relevância do acesso, por particulares, a bases de dados públicas para prestar serviços de interesse da sociedade, como, por exemplo, prevenção a fraude e ao superendividamento.

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

- I - finalidade específica do tratamento;
- II - forma e duração do tratamento;
- III - identificação do responsável;
- IV - informações de contato do responsável;
- V - sujeitos ou categorias de sujeitos para os quais os dados podem ser comunicados e o âmbito de sua difusão;
- VI - responsabilidades dos agentes que realizarão o tratamento; e
- VII - direitos do titular, com menção explícita à possibilidade de:
  - a) acessar os dados, retificá-los ou revogar o consentimento, por procedimento gratuito e facilitado;
  - b) denunciar ao órgão competente o descumprimento de disposições desta Lei; e
  - c) não fornecer o consentimento, na hipótese em que o consentimento é requerido, mediante o fornecimento de informações sobre as consequências da negativa.

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

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

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

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

§ 5º O órgão competente poderá dispor sobre os meios referidos no § 4º.

**Inclusão de novo § 2º do artigo 8º, renumerando-se o atual e os subsequentes,** para que finalidades adicionais possam ser informadas aos titulares, assegurando-se a eles o direito de revogar o consentimento nos casos em que este seja requerido. Sugere-se, para tanto, a seguinte redação:

*“§ 2º O responsável pelo tratamento deverá informar previamente ao titular eventual finalidade adicional para o tratamento da informação prevista no inciso I, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração”.*

**Justificativa:** em atenção ao princípio da finalidade, sugerimos que o responsável pelo tratamento seja obrigado a dar ciência de eventual nova finalidade do tratamento ao titular para que, querendo, possa exercer a faculdade de retificar os dados ou revogar o consentimento. Isso porque não se altera a finalidade inicial, motivo pelo qual se deve preservar o consentimento já obtido para este sem, com isso, criar ônus adicional. Esta medida visa a trazer mais fluidez para o mercado, sem, no entanto, retirar o poder do titular de controlar as suas informações.

**Modificação do atual § 2º do artigo 8º,** para que se admita a divulgação dos novos dados de contato do responsável pelo tratamento mediante disponibilização em seu sítio eletrônico, da seguinte forma:

*“§ 2º Em caso de alteração de informação referida no inciso IV do caput, o responsável deverá comunicar ao titular ou disponibilizar em seu sítio eletrônico as informações de contato atualizadas.”*

**Justificativa:** como as informações de contato do responsável pelo tratamento se destinam a possibilitar a sua localização pelo titular, qualquer forma de disponibilização ostensiva deve ser útil a este propósito. Entendemos que a informação disponível em meio eletrônico é de mais fácil localização e acesso pelo titular do que uma informação que lhe seja comunicada apenas uma vez. Por esta razão, sugerimos a inclusão acima.

**Supressão do atual § 3º do artigo 8º.**

**Justificativa:** em atenção aos requisitos previstos neste projeto de lei para a coleta do consentimento do titular, este deve ser claramente informado, dentre outros, sobre a duração do tratamento dos dados pessoais. Logo, é inequívoca a sua ciência e concordância com o tratamento continuado de seus dados pessoais ao consentir com a sua realização. É assegurado ao titular, ainda, o direito de revogar seu consentimento a qualquer tempo.

Logo, não se vislumbra nenhum benefício razoável e proporcional, para o titular, que justifique a providência adicional de, de tempos em tempos, ser comunicado de que o tratamento com o qual ele consentiu de forma informada e válida continua a ser realizado. Não decorre, desta providência, nenhuma proteção adicional ao titular de dados pessoais que justifique o ônus atribuído ao responsável para a sua obtenção.

Veja-se que a lei deve preservar, de forma equilibrada, a proteção dos titulares, a sua liberdade de escolha, o livre exercício empresarial dos responsáveis pelo tratamento e o desenvolvimento econômico e social do país.

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

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

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

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

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

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

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

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

**Comentário sobre revogação do consentimento:** a possibilidade de revogação do consentimento é inerente ao direito de controle do titular sobre os seus dados pessoais. Deve-se ter claro, contudo, que nos casos em que o tratamento de dados pessoais é condição para a prestação de um serviço ou fornecimento de um produto, a revogação naturalmente implicará a sua cessação, conforme o caso, consequência esta que não pode ser confundida com ônus para o titular. Vale destacar, ainda, que, em observância ao ato jurídico perfeito, a revogação do consentimento não deve afetar a legalidade e a validade do tratamento de dados pessoais realizados enquanto vigente o referido consentimento. Por fim, a revogação do consentimento também não deverá afetar a permanência da anotação do inadimplemento de obrigações pelo titular mediante solicitação do credor a bancos de dados de proteção ao crédito, devidamente comunicada ao titular nos termos do art. 43 da Lei nº 8.078/90 – Código de Defesa do Consumidor, enquanto não houver o adimplemento da obrigação ou o decurso do prazo previsto no § 1º do art. 43 do CDC, o que ocorrer primeiro.

**Modificação do § 2º do art. 9º**, a fim de substituir o termo “responsável” por “fonte”, passando a constar a seguinte redação:

*“§ 2º Cabe à fonte o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.”*

**Justificativa:** trata-se de adequação de acordo com a sugestão de inclusão prevista no artigo 5º. O responsável pode ser o gestor do banco de dados ou a fonte, no entanto, cabe à fonte, que poderá ser ou não a responsável pelo tratamento, a coleta e o fornecimento dos dados para determinada finalidade.

**Modificação do § 4º do art. 9º,** passando a constar com a seguinte redação:

*“§ 4º O consentimento deverá se referir a finalidades devidamente informadas ao titular para o tratamento de dados pessoais.”*

**Justificativa:** o termo “autorizações genéricas” se mostra extremamente vago, gerando insegurança jurídica sobre sua definição. Ademais, com a evolução do ambiente digital e o tratamento dos dados dele provenientes, como no caso do big data, a obrigação de determinação prévia da finalidade exata da coleta de dados pode ser extremamente difícil, embora seja viável estabelecer limites que devem ser observados para tanto.

Vale dizer que o direito de controle sobre os dados pessoais, ao decorrer dos direitos à intimidade e à vida privada, converte-se em direito personalíssimo e, como tal, não merece ser limitado pelo Estado. Compete somente ao titular exercê-lo sob as condições que entender adequadas, evidentemente após terem sido fornecidas a ele suficientes informações para esta tomada de decisão, tratando-se com rigor eventual abuso ou não atendimento dos benefícios originalmente informados a ele.

**Supressão do § 6º do art. 9º.**

**Justificativa:** uma vez que o titular possui o direito de revogar o seu consentimento a qualquer tempo, entendemos que não há prejuízo a ele se, em caso de alteração em qualquer das informações referenciadas nos incisos I, II, III ou V do artigo 8º, for comunicado a respeito para, querendo, revogar o seu consentimento.

Reitera-se a importância de garantir ao titular os meios necessários para controlar o tratamento de seus dados pessoais. Porém, este direito deve estar alinhado ao princípio da razoabilidade, não se impondo condições que terminem por inviabilizar e tornar inócua a importante proteção que lhe será conferida com a aprovação da lei de proteção de dados pessoais.

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

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

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

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

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

**Modificação do § 1º**, passando a constar a seguinte redação: *“O legítimo interesse deve ser compatível com a finalidade informada ao titular para o tratamento de seus dados, de acordo com o disposto no art. 6º, inciso II.”*

**Justificativa:** Conforme informado na alteração sugerida para o art. 6º, II, adequação é, a rigor, a correspondência entre o que é proposto e o que é efetivamente realizado. Logo, a “legítima expectativa do titular” deve corresponder aos fins que lhe foram informados e para os quais consentiu com o tratamento de seus dados pessoais. Trata-se de substituição do conceito subjetivo por uma análise objetiva da correspondência entre a finalidade informada ao titular e aquela efetivamente dada às informações.

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

I - com fornecimento de consentimento livre, inequívoco, informado, expresso e específico pelo titular:

- a) mediante manifestação própria, distinta da manifestação de consentimento relativa a outros dados pessoais; e
- b) com informação prévia e específica sobre a natureza sensível dos dados a serem tratados, com alerta quanto aos riscos envolvidos no seu tratamento.

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

- a) cumprimento de uma obrigação legal pelo responsável;
- b) tratamento e uso compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
- c) realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
- d) exercício regular de direitos em processo judicial ou administrativo;
- e) proteção da vida ou da incolumidade física do titular ou de terceiro; ou
- f) tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias.

§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais capaz de revelar dados pessoais sensíveis.

§ 2º O tratamento de dados pessoais sensíveis não poderá ser realizado em detrimento do titular, ressalvado o disposto em legislação específica.

§ 3º O disposto na alínea “c” do inciso II não se aplica caso as atividades de pesquisa estejam vinculadas a qualquer das seguintes atividades:

I - comercial;

II - de administração pública, quando a pesquisa não for a atividade principal ou legalmente estabelecida do órgão; ou

III - relativa à investigação criminal ou inteligência,

§ 4º Nas hipóteses do parágrafo anterior, sempre que possível, será garantida a anonimização dos dados pessoais.

§ 5º Nos casos de aplicação do disposto nas alíneas “a” e “b” do inciso II pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do art. 24.

Art. 12. O órgão competente poderá estabelecer medidas adicionais de segurança e de proteção aos dados pessoais sensíveis, que deverão ser adotadas pelo responsável ou por outros agentes do tratamento, ou solicitar a apresentação de relatório de impacto à privacidade.

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

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

**Modificação do § 1º**, para que seja admitido o uso dos dados anonimizados para a formação de perfil comportamental. Sugere-se, para tanto, a seguinte redação: “Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, os dados utilizados para a formação do perfil comportamental de uma determinada pessoa natural, se identificada.”

**Justificativa:** o principal propósito da anonimização é impedir que o tratamento de dados pessoais seja capaz de causar qualquer dano a uma pessoa ou grupo de pessoas naturais. Desta forma, ao anonimizar-se os dados, é possível analisar e estudar as informações que se pode extrair deles para inovação e desenvolvimento econômico e social. Veja-se que tais dados não deixam de merecer a adequada proteção quanto ao seu armazenamento para evitar o acesso indevido ou a desanonimização. Porém, o seu tratamento de forma anônima não é capaz de gerar prejuízo a qualquer pessoa determinada ou determinável enquanto não desanonimizado, razão pela qual não se justifica obstar a sua utilização para a formação de perfis comportamentais e, com isso, privar os próprios titulares do desenvolvimento econômico e tecnológico que pode resultar de tais estudos.

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

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

**Modificação do § 3º**, para que se defina melhor o que se entende por publicidade, considerando-se o fato de que os dados são anonimizados e o seu tratamento não pode implicar prejuízo a qualquer titular identificado ou identificável enquanto se der de forma anônima. Sugere-se, para tanto, a seguinte redação: “O compartilhamento e o uso que se faz de dados anonimizados deve ser informado ao órgão competente, que pode solicitar ao responsável relatório de impacto à privacidade referente aos riscos de reversão do processo de anonimização e demais aspectos de seu tratamento.”

**Justificativa:** a principal premissa para uma legislação que atenda adequadamente ao propósito a que se propõe é o equilíbrio, ou seja, a lei deve ser capaz de proteger direitos e, para tanto, criar apenas as obrigações necessárias para esta finalidade, em conformidade com os princípios da razoabilidade e da proporcionalidade.

O projeto de lei em análise prevê a designação de um órgão competente para tratar da proteção de dados pessoais, ao qual competirá analisar os procedimentos adotados pelos responsáveis pelo tratamento e recomendar as medidas necessárias à proteção de sua privacidade. Logo, a publicidade e transparência sobre o tratamento de dados anonimizados deve ser concedida a tal órgão, de modo que não haja custos e medidas operacionais desnecessárias ao dar-se ciência de processos complexos para o público em geral que sequer poderá avaliar se disso decorre qualquer prejuízo ou não, haja vista a anonimização em si.

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

## Seção II

### Término do tratamento

Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

II - fim do período de tratamento;

III - comunicação do titular, inclusive no exercício do seu direito de revogação do consentimento conforme disposto no art. 9º, § 5º; ou

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

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

#### **Supressão do parágrafo único do artigo 15.**

**Justificativa:** uma vez que o tratamento dos dados pessoais pressupõe o consentimento informado do titular civilmente capaz, inclusive no que tange à sua duração, sugerimos a supressão do parágrafo único, já que, caso o titular não queira mais que seus dados sejam tratados pelo período com o qual concordou inicialmente, é assegurado ele revogar o consentimento a qualquer tempo. Torna-se, assim, desnecessário o estabelecimento de prazos pelo órgão competente, o que poderia, inclusive, deixar de abranger uma das diversas finalidades que podem justificar o tratamento de dados pessoais. Novamente, busca-se preservar o equilíbrio das relações sociais que se pretende regulamentar, estabelecendo obrigações adequadas e proporcionais aos direitos que se visa a assegurar.

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

I - cumprimento de obrigação legal do responsável;

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

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

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

**Adição do inciso IV**, para prever a manutenção também para fins de auditoria e atendimento a ordens judiciais, nos seguintes termos: *“atendimento a auditorias internas e ordens judiciais para o fornecimento de dados pessoais tratados pelo responsável.”*

**Justificativa:** é necessário que os responsáveis pelo tratamento de dados pessoais possam controlar os seus processos internos, assegurando a sua qualidade e, se necessário, subsidiar informações para a defesa de direitos dos titulares mesmo após o término do prazo previsto para o tratamento de dados pessoais ou exercer o seu direito constitucional de defesa. Por isso, para tais propósitos exclusivos, também se revela importante admitir a manutenção dos dados pessoais sem a sua divulgação a terceiros salvo mediante ordem judicial expressa.

### CAPÍTULO III DOS DIREITOS DO TITULAR

Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais, garantidos os direitos fundamentais de liberdade, intimidade e privacidade, nos termos desta Lei.

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

I - confirmação da existência de tratamento;

II - acesso aos dados;

III - correção de dados incompletos, inexatos ou desatualizados;

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

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

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

e

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

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

§ 2º Os direitos previstos neste artigo serão exercidos mediante requerimento do titular a um dos agentes de tratamento, que adotará imediata providência para seu atendimento.

§ 3º Em caso de impossibilidade de adoção imediata da providência de que trata o § 2º, o responsável enviará ao titular, em até sete dias, contados da data do recebimento do requerimento, resposta em que poderá:

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

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

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

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

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

I - em formato simplificado, imediatamente; ou

II - por meio de declaração clara e completa, que indique a origem dos dados, a data de registro, os critérios utilizados e a finalidade do tratamento, fornecida no prazo de até sete dias, contado da data do requerimento do titular.

§ 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.

§ 2º As informações e os dados poderão ser fornecidos, a critério do titular:

I - por meio eletrônico, seguro e idôneo para tal fim; ou

II - sob forma impressa, situação em que poderá ser cobrado exclusivamente o valor necessário ao ressarcimento do custo dos serviços e dos materiais utilizados.

§ 3º Quando o tratamento tiver origem no consentimento do titular ou em um contrato, o titular poderá solicitar cópia eletrônica integral dos seus dados pessoais em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

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

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

**Modificação do § 2º e supressão do § 3º**, nos seguintes termos:

*“§ 2º As informações e dados poderão ser fornecidos, a critério do titular, pelos meios a seguir previstos, podendo ser cobrado exclusivamente o custo dos serviços e materiais para fornecimento desde que assegurado ao titular ao menos um meio de acesso gratuito:*

*I – meio eletrônico, seguro e idôneo para tal fim; ou*

*II – meio impresso.”*

**Justificativa:** a atual redação do § 2º contempla a possibilidade de cobrança dos custos apenas para o fornecimento de dados na forma impressa. Contudo, não se pode deixar de reconhecer que o meio eletrônico também gera custos para o responsável pelo tratamento de dados, tais como provedor de conexão à internet, desenvolvimento e manutenção de sistemas, ferramentas de identificação e gestão de acessos, além de pessoal especializado para estruturar e administrar o procedimento proposto.

Com relação às empresas que possuem bancos de dados e exploram essa atividade de maneira profissional, devemos destacar que, embora possuam caráter público haja vista a sua elevada importância na conjuntura comercial e econômica do País, tratam-se de companhias privadas que não possuem aporte

governamental para a manutenção de seus processos e, portanto, precisam ter assegurada a sua capacidade de melhor alocação de recursos sem que, com isso, seja prejudicado o acesso dos titulares às suas informações.

Para efeitos de comparação, podemos destacar os trabalhos realizados pelos cartórios, que também cuidam de anotações e registros de títulos de inadimplência e não oferecem gratuidade pelos seus serviços. Ainda que alguns estados da Federação liberem o credor do pagamento de custas para a realização de protestos, este custo é integralmente transferido ao devedor, sendo adicionado ao valor da dívida no momento da regularização.

Já os bancos de dados de proteção ao crédito, entes privados que exploram atividade empresarial ordenada, permitida pela Constituição Federal e pelo Código de Defesa do Consumidor, sem qualquer custo para os consumidores no momento da regularização de suas pendências, asseguram atualmente o acesso gratuito e ilimitado dos consumidores às suas informações, cabendo-lhes apenas o direito de escolher os canais de atendimento. Deveria, portanto, ser-lhes assegurado ao menos o direito ao reembolso de tais custos e à definição dos canais em que será observada a gratuidade.

Vale ponderar, ainda, que face ao alto volume de fraudes no país e à indústria do dano moral, a concessão de acesso ilimitado gratuito às informações via internet pode dar ensejo a ações temerárias, mediante a apresentação de informações desatualizadas ou manipuladas aos potenciais credores, como se tratasse de um "salvo conduto" para comprar e contratar, aumentando, conseqüentemente, o número de fraudes. Por esses motivos, sugeriu-se também a supressão do § 3º do artigo em análise.

Vale destacar a enorme quantidade de fraudes atualmente existentes nos meios eletrônicos, cada vez mais sofisticadas e frequentes, as quais demandam vultuosos investimentos para a sua identificação e prevenção, reforçando-se a necessidade de que, para a implementação de conveniência desta natureza, possam os bancos de dados ter liberdade de estabelecer uma contrapartida não apenas legítima, mas necessária nas relações econômicas para preservar a sua estabilidade financeira e a sua continuidade no mercado em que atuam.

**Exclusão do § 4º**, para que se preserve a possibilidade de livre definição do formato de fornecimento dos dados.

**Justificativa:** a lei deve obedecer ao princípio da razoabilidade. Nesta linha, uma vez que o projeto já determina que os dados devem ser armazenados em formato que facilite o direito de acesso à informação, bem como o dever de os responsáveis pelo tratamento os fornecerem aos titulares solicitantes, compete aos responsáveis, a depender da forma como tenham organizado seus bancos de dados, definir o formato que entenderem mais adequado para o entendimento das informações pelo titular. Não se vislumbra benefício que possa advir desta ingerência estatal na atividade privada que justifique a adoção da medida.

Art. 20. O titular dos dados tem direito a solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive as decisões destinadas a definir o seu perfil ou avaliar aspectos de sua personalidade.

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

**Modificação do parágrafo único**, a fim de melhor estabelecer os critérios da decisão automatizada e evitar, de fato, a violação aos segredos comercial e industrial:

*“O responsável deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos principais critérios considerados para a decisão automatizada, respeitados os segredos comercial e industrial.”*

**Justificativa:** esta modificação visa a conciliar o direito do titular à proteção de seus dados pessoais, o qual deve indubitavelmente ser respeitado, com a liberdade empresarial. Logo, sugere-se que, no tocante não aos dados em si, mas aos critérios considerados para as decisões automatizadas, sejam divulgados apenas os principais, assegurando, assim, a manutenção de diferenciais competitivos na análise e protegendo de fato os segredos empresarial e industrial sem prejuízo ao direito de acesso à informação que assiste aos titulares. Sugere-se, ainda, que a revisão de que se trata seja endereçada aos responsáveis pela decisão, quando estes foram diferentes dos responsáveis pelo tratamento dos dados.

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

Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo individual ou coletivamente, na forma do disposto na Lei nº 9.507, de 12 de novembro de 1997, nos art. 81 e art. 82 da Lei nº 8.078, de 11 de setembro de 1990, na Lei nº 7.347, de 24 de julho de 1985, e nos demais instrumentos de tutela individual e coletiva.

#### CAPITULO IV

#### DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

##### Seção I

##### Tratamento de Dados Pessoais pelo Poder Público

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

Art. 24. 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, nos termos do art. 40.

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

Art. 25. As empresas públicas e 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. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios da proteção de dados pessoais elencados no art. 6º desta Lei.

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

**Modificação do parágrafo único do artigo 26**, sugerindo-se que passe a constar com a seguinte redação:

*“É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto em casos de execução descentralizada de atividade pública que o exija e exclusivamente para este fim específico e determinado, bem como para atender interesse público e geral relevante, nos termos do artigo 31, § 3º, V, da Lei nº 12.527, de 2011.”*

**Justificativa:** o art. 5º, inc. XXXIII, da Constituição Federal, dispõe que “todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado”.

A Lei de Acesso a Informação (Lei nº 12.527/2011), ao regulamentar o direito fundamental à informação, estabeleceu as seguintes diretrizes: “I - observância da publicidade como preceito geral e do sigilo como exceção; II - divulgação de informações de interesse público, independentemente de solicitações; III - utilização de meios de comunicação viabilizados pela tecnologia da informação; IV - fomento ao desenvolvimento da cultura de transparência na administração pública; V - desenvolvimento do controle social da administração pública”.

Cabe, portanto, aos órgãos integrantes da Administração Pública assegurar o acesso aos dados públicos a todos que lhe solicitarem, inclusive divulgando-os independentemente de solicitação, resguardando-se, por óbvio, os dados cujo sigilo é imprescindível para a segurança da sociedade e do Estado.

Logo, não havendo prejuízo para a segurança da sociedade e do Estado, não vislumbramos óbice algum para o fornecimento massivo de dados, pelos órgãos da Administração Pública, para particulares que poderiam acessá-los livremente pela internet, por exemplo.

A possibilidade da celebração de convênio específico entre particulares e órgãos da Administração Pública pode, ainda, trazer mais segurança jurídica para os titulares dos dados e controle quanto à sua atualização e ao seu uso adequado, haja vista a possibilidade de prever-se regras específicas para o acesso em grandes quantidades. Logo, não há sequer que se falar em autorização da autoridade de garantia, haja vista a publicidade imanente dos dados a serem cedidos.

Neste sentido, destaca-se a recente decisão do Superior Tribunal de Justiça que, em julgamento dos Recursos Especiais avocados como Repetitivos nºs 1444469-DF e 1344352-SP, decidiu pela desnecessidade de comunicar-se aos consumidores a inclusão de informações provenientes de fonte pública em bancos de dados de proteção ao crédito.

Vale destacar a relevância do acesso, por particulares, a bases de dados públicas para prestar serviços de interesse da sociedade, como, por exemplo, prevenção a fraude e ao superendividamento.

Art. 27. A comunicação e 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. 24.

**Modificação do “caput” do art. 27**, para que sujeite apenas os dados sujeitos a acesso público restrito às disposições de que trata. Sugere-se, para tanto, a seguinte redação:

*“A comunicação e a transferência de dados pessoais de acesso público restrito entre pessoa jurídica de direito público a pessoa de direito privado será informada ao órgão competente e dependerá de consentimento do titular, exceto:”*

**Justificativa:** segundo o art. 5º, inc. XXXIII, da Constituição Federal, dispõe que “todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado”.

A Lei de Acesso a Informação (Lei nº 12.527/2011), ao regulamentar o direito fundamental à informação, estabeleceu as seguintes diretrizes:

I - observância da publicidade como preceito geral e do sigilo como exceção;

II - divulgação de informações de interesse público, independentemente de solicitações;

III - utilização de meios de comunicação viabilizados pela tecnologia da informação;

IV - fomento ao desenvolvimento da cultura de transparência na administração pública;

V - desenvolvimento do controle social da administração pública”.

Cabe, portanto, aos órgãos integrantes da Administração Pública assegurar o acesso aos dados públicos a todos que lhe solicitarem, inclusive divulgando-os independentemente de solicitação, resguardando-se, por óbvio, os dados cujo sigilo é imprescindível para a segurança da sociedade e do Estado.

Logo, não há sequer que se falar em autorização da autoridade de garantia, haja vista a publicidade imanente dos dados a serem cedidos.

Neste sentido, destaca-se a recente decisão do Superior Tribunal de Justiça que, em julgamento dos Recursos Especiais avocados como Repetitivos nºs 1444469-DF e 1344352-SP, decidiu pela desnecessidade de comunicar-se aos consumidores a inclusão de informações provenientes de fonte pública em bancos de dados de proteção ao crédito.

Vale destacar a relevância do acesso, por particulares, a bases de dados públicas para prestar serviços de interesse da sociedade, como, por exemplo, prevenção a fraude e ao superendividamento.

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

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

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

## **Seção II**

### **Responsabilidade**

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

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

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

## **CAPÍTULO V**

### **DA TRANSFERÊNCIA INTERNACIONAL DE DADOS**

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

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

II - quando a transferência for necessária para a cooperação judicial internacional entre órgãos públicos de inteligência e de investigação, de acordo com os instrumentos de direito internacional;

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

IV - quando o órgão competente autorizar a transferência;

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

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

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

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

- I - as normas gerais e setoriais da legislação em vigor no país de destino;
- II - a natureza dos dados;
- III - a observância dos princípios gerais de proteção de dados pessoais previstos nesta Lei;
- IV - a adoção de medidas de segurança previstas em regulamento; e
- V - as outras circunstâncias específicas relativas à transferência.

Art. 34. A autorização referida no inciso IV do **caput** do art. 33 será concedida quando o responsável pelo tratamento apresentar garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular, apresentadas em cláusulas contratuais aprovadas pelo órgão competente para uma transferência específica, em cláusulas contratuais padrão ou em normas corporativas globais, nos termos do regulamento.

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

§ 2º Os responsáveis pelo tratamento que fizerem parte de um mesmo grupo econômico ou conglomerado multinacional poderão submeter normas corporativas globais à aprovação do órgão competente, obrigatórias para todas as empresas integrantes do grupo ou do conglomerado, a fim de obter permissão para transferências internacionais de dados dentro do grupo ou do conglomerado sem necessidade de autorizações específicas, observados os princípios gerais de proteção e os direitos do titular.

§ 3º Na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação do órgão competente, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento.

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

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

**Modificação do artigo 35**, com a inclusão dos incisos I e II, nos seguintes termos:

*“Art. 35. O cedente e o cessionário respondem pelos danos decorrentes do tratamento de dados, independentemente do local onde estes se localizem, devendo ser apuradas as respectivas responsabilidades, cabendo:*

*I – ao cedente, a responsabilidade pela integridade dos dados pessoais transmitidos tais como coletados e pela comunicação de eventuais alterações nos dados ou no consentimento ao cessionário;*

*II – ao cessionário, a integridade dos dados pessoais tais como transmitidos pelo cedente, pelo seu tratamento em conformidade com o consentimento e pela adequação dos dados de acordo com posteriores comunicações do cedente.”*

**Justificativa:** o cedente e o cessionário, por serem pessoas jurídicas diversas e independente, não exercem controle sobre as atividades um do outro, conforme decorre do princípio constitucional da liberdade empresarial estatuído no artigo 170 da Constituição Federal.

Portanto, não é razoável atribuir-se responsabilidade solidária entre cedente e cessionário pois estes não possuem poder de supervisão e controle que lhes permita evitar os prejuízos que serão obrigados a reparar.

Convém citar o exemplo do Cadastro Positivo, em que a responsabilidade objetiva e solidária entre fontes, consulentes e bancos de dados tem representado um importante entrave para a implementação exatamente em razão do argumento acima exposto.

Este projeto pode, outrossim, estabelecer as obrigações das partes para que cada qual responda pelos danos a que der causa, considerando-se, ainda, que esta proposta já prevê a necessidade de o titular consentir com a interconexão de dados, ou seja, ele tem ciência inequívoca e poder de controle sobre o eventual compartilhamento de suas informações.

Por esses motivos, sugere-se a distribuição de responsabilidades apresentadas neste artigo, que endereça, de forma equilibrada e abrangente, os atos sujeitos à esfera de atuação de cedente e cessionário.

## CAPÍTULO VI

### DOS AGENTES DO TRATAMENTO DE DADOS PESSOAIS

#### Seção I

#### Responsável e operador

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

**Modificação do art. 36,** substituindo-se o termo “operador” por “gestor de banco de dados”, passando a constar da seguinte forma: *“São agentes do tratamento de dados pessoais o responsável e o gestor de banco de dados.”*

**Justificativa:** conforme sugestão para alteração do artigo 5º, IX (definição de operador), trata-se de adequação de nomenclatura àquela já empregada em diploma legal vigente (Lei do Cadastro Positivo).

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

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

**Modificação do art. 37,** substituindo-se o termo “operador” por “gestor de banco de dados”, passando a constar com a seguinte redação: *“O responsável e o gestor de banco de dados devem manter registro das operações de tratamento de dados pessoais que realizarem.”*

**Justificativa:** conforme sugestão para alteração do artigo 5º, IX (definição de operador), trata-se de adequação de nomenclatura àquela já empregada em diploma legal vigente (Lei do Cadastro Positivo).

Art. 38. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo responsável, que verificará a observância das próprias instruções e das normas sobre a matéria.

**Modificação do art. 38,** substituindo-se o termo “operador” por “gestor de banco de dados”, passando a constar com a seguinte redação:

*“O gestor de banco de dados deverá realizar o tratamento segundo as instruções fornecidas pelo responsável, que verificará a observância das próprias instruções e das normas sobre a matéria.”*

**Justificativa:** Conforme sugestão para alteração do artigo 5º, IX (conceito de operador), trata-se de adequação de nomenclatura àquela já empregada em diploma legal vigente (Lei do Cadastro Positivo).

Art. 39. O órgão competente poderá determinar ao responsável que elabore relatório de impacto à privacidade referente às suas operações de tratamento de dados, nos termos do regulamento.

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

**Modificação do art. 40,** para que passe a prever também a hipótese de consentimento já manifestado em qualquer dos atos de tratamento de dados:

*“A comunicação de dados pessoais entre responsáveis ou gestores de bancos de dados de direito privado dependerá do consentimento do titular, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei e eventual concordância já manifestada em qualquer momento do tratamento dos dados.”*

**Justificativa:** em atenção aos princípios da razoabilidade e da proporcionalidade, sugere-se que, caso o titular já tenha consentido com a referida comunicação em qualquer momento do tratamento de dados pessoais, não seja necessário que manifeste, novamente, a sua concordância. Alternativamente, entendemos que possa ser adotado também o procedimento de comunicação ao titular sobre a comunicação dos dados entre responsáveis ou gestores de bancos de dados, se não abrangida no consentimento original, a fim de que o titular possa exercer o controle sobre a circulação de seus dados pessoais, princípio este que norteia esta proposta.

Se acolhida esta sugestão, sugere-se ainda a revisão dos artigos subsequentes deste Capítulo para que sejam norteados pelos mesmos princípios de razoabilidade e eficiência na coleta do consentimento dos titulares de dados pessoais e/ou de comunicação.

## Seção II

### Encarregado pelo tratamento de dados pessoais

Art. 41. O responsável deverá indicar um encarregado pelo tratamento de dados pessoais.

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente de forma clara e objetiva, preferencialmente no sítio eletrônico do responsável.

§ 2º As atividades do encarregado consistem em:

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

II - receber comunicações do órgão competente e adotar providências;

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

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

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

### Seção III

#### Responsabilidade e ressarcimento de danos

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

Parágrafo único. O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

**Modificação do art. 42**, a fim de trazer para este projeto de lei a distribuição de responsabilidades já delimitada pela jurisprudência ao analisar a responsabilidade das partes no tratamento dos dados de consumo para a proteção ao crédito:

*“Todo aquele que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, é obrigado a repará-lo, considerando-se que compete:*

*a) aos gestores de bancos de dados, a integridade dos dados pessoais tais como recebidos;*

*b) às fontes, a veracidade e a atualização dos dados pessoais que fornecerem;*

*c) aos consulentes, a utilização dos dados pessoais apenas para os fins para os quais lhes sejam fornecidos.”*

**Justificativa:** Nos casos em que a legislação pátria prevê a responsabilidade objetiva, como para as relações de consumo, admite-se excludentes, a exemplo do art. 14 do Código de Defesa do Consumidor, precedente este importante de ser aproveitado e replicado neste projeto de lei. Sugere-se, portanto, que prevaleça a regra geral da responsabilidade subjetiva do Código Civil, com as melhorias acima, consistentes na distribuição das responsabilidades entre as partes, o que contribui para melhor orientar eventuais ações destinadas ao ressarcimento de dados, aplicando-se a legislação específica, por exemplo, consumerista, quando houver.

Outra importante melhoria trazida para este artigo consiste na atribuição de responsabilidade para outras partes envolvidas no tratamento de dados pessoais, como fontes e consulentes, na qualidade de

beneficiários das informações contidas nos bancos de dados e que, portanto, também devem cuidar da sua utilização adequada.

Por fim, vale dizer que sugerimos no artigo 5º a substituição do termo "operador" (inciso IX) por "gestor de banco de dados", adequando-se a nomenclatura àquela já empregada em diploma legal vigente (Lei do Cadastro Positivo), bem como a inclusão de dois incisos (VII e VIII), que incluem os termos "fonte" e "consulente", de modo que seja possível a adequada identificação dos responsáveis e atribuição de responsabilidades, conforme aqui proposto.

Art. 43. A eventual dispensa da exigência do consentimento não desobriga os agentes do tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

Art. 44. Nos casos que envolvem a transferência de dados pessoais, o cessionário ficará sujeito às mesmas obrigações legais e regulamentares do cedente, com quem terá responsabilidade solidária pelos danos eventualmente causados.

Parágrafo único. A responsabilidade solidária não se aplica aos casos de tratamento realizado no exercício dos deveres de que trata a Lei nº 12.527, de 2011, relativos à garantia do acesso a informações públicas.

**Modificação do art. 44**, substituindo-se a responsabilidade solidária pelos danos eventualmente causados pela necessária apuração das respectivas responsabilidades”, bem como sugere-se a **supressão do parágrafo único**:

*“Art. 44. Nos casos que envolvem a transferência de dados pessoais, o cessionário ficará sujeito às mesmas obrigações legais e regulamentares do cedente, devendo ser apuradas as respectivas responsabilidades pelos danos eventualmente causados.”*

**Justificativa:** o cedente e o cessionário, por serem pessoas jurídicas diversas e independentes, não exercem controle sobre as atividades um do outro, conforme decorre do princípio constitucional da liberdade empresarial estatuído no artigo 170 da Constituição Federal.

Portanto, não é razoável atribuir-se responsabilidade solidária entre cedente e cessionário pois estes não possuem poder de supervisão e controle que lhes permita evitar os prejuízos que serão obrigados a reparar.

Mais uma vez, convém citar o exemplo do Cadastro Positivo, em que a responsabilidade objetiva e solidária entre fontes, consulentes e bancos de dados tem representado em importante entrave para a implementação exatamente em razão do argumento acima exposto.

Este projeto de lei pode, outrossim, estabelecer as obrigações das partes para que cada qual responda pelos danos a que der causa, considerando-se, ainda, que esta proposta já prevê a necessidade de o titular consentir com a interconexão de dados, ou seja, ele tem ciência inequívoca e poder de controle sobre o eventual compartilhamento de suas informações.

Por esses motivos, sugere-se a distribuição de responsabilidades aqui apresentada, que endereça, de forma equilibrada e abrangente, os atos sujeitos à esfera de atuação de cedente e cessionário.

## **Seção I**

### **Segurança e sigilo de dados**

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

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

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

Art. 46. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se ao dever de sigilo em relação aos dados pessoais, mesmo após o seu término.

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

Parágrafo único. A comunicação será feita em prazo razoável, conforme definido pelo órgão competente, e deverá mencionar, no mínimo:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - a indicação das medidas de segurança utilizadas para a proteção dos dados, inclusive procedimentos de encriptação;

IV - os riscos relacionados ao incidente;

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

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

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

I - pronta comunicação aos titulares;

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

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

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

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

**Modificação do §1º**, para prever também a possibilidade de controles compensatórios que mitiguem o risco de acesso indevido às informações, Sugere-se, para isso, a seguinte redação:

“No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis para terceiros não autorizados a acessá-los e/ou controles compensatórios que mitiguem o risco de acesso indevido às informações.”

**Justificativa:** em alguns casos, tornar os dados “ininteligíveis”, por criptografia ou outro tipo de tecnologia, não é operacionalmente viável, de modo que se deve admitir também a adoção de outras medidas que ao menos mitiguem o risco de acesso indevido, tais como uma robusta gestão de vulnerabilidades em aplicações e infraestrutura e o ferramentas de proteção de borda, amplamente adotadas e hábeis a garantir mais segurança às informações. Veja-se que, embora caiba ao órgão competente a avaliação dos incidentes e das medidas a serem tomadas, a lei deverá assegurar-lhe suficiente margem de atuação para que possa executar este mister e praticar atos administrativos em consonância com os princípios da discricionariedade e da legalidade.

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

## **Seção II**

### **Boas práticas**

Art. 50. Os responsáveis pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas que estabeleçam 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 pelo órgão competente.

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

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

- I - multa simples ou diária;
- II - publicização da infração;
- III - anonimização dos dados pessoais;

- IV - bloqueio dos dados pessoais;
- V - suspensão de operação de tratamento de dados pessoais;
- VI - cancelamento dos dados pessoais; e
- VII - suspensão de funcionamento de banco de dados.

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

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

§ 3º O disposto nos incisos III a VII do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 1990, e na Lei nº 8.429, de 1992.

**Modificação do § 3º do art. 52**, para que a publicização da infração seja aplicável também às entidades e aos órgãos públicos:

*“O disposto nos incisos II a VII do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 1990, e na Lei nº 8.429, de 1992.”*

**Justificativa:** não se vislumbra motivo pelo qual a penalidade do item II não possa ser aplicada também aos órgãos públicos. Tais órgãos abrigam uma vasta quantidade de dados pessoais e, caso haja descumprimento dos preceitos legais no tratamento desses dados, é direito da coletividade conhecê-los, posto que pode ser igualmente afetada. Recomenda-se, portanto, que seja aplicável a penalidade de publicização da infração assim como ocorre em relação às entidades privadas.

## Seção II

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

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

- I - zelar pela proteção dos dados pessoais, nos termos da legislação;
- II - elaborar diretrizes para uma Política Nacional de Proteção de Dados Pessoais e Privacidade;
- III - realizar auditoria nos tratamentos de dados pessoais e processos envolvidos com dados pessoais visando garantir a sua conformidade aos princípios e regras desta Lei;
- IV - promover entre a população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e as medidas de segurança;
- V - promover estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;
- VI - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais;
- VII - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;

- VIII - dispor sobre as formas pelas quais se dará a publicidade das operações de tratamento;
- IX - solicitar, a qualquer momento, às entidades do Poder Público que realizem operações de tratamento de dados pessoais, informe específico sobre o âmbito, natureza dos dados e demais detalhes do tratamento realizado, podendo emitir parecer técnico complementar para garantir o cumprimento desta Lei;
- X - estabelecer normas complementares para as atividades de comunicação de dados pessoais;
- XI - elaborar relatórios anuais acerca de suas atividades;
- XII - editar normas sobre proteção de dados pessoais e privacidade; e
- XIII - realizar demais ações dentro de sua esfera de competência, inclusive as previstas nesta Lei e em legislação específica.

Art. 54. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto por quinze representantes titulares, e seus respectivos suplentes, dos seguintes órgãos:

- I - sete representantes do Poder Executivo federal;
- II - um representante indicado pelo Congresso Nacional;
- III - um representante indicado pelo Conselho Nacional de Justiça;
- IV - um representante indicado pelo Conselho Nacional do Ministério Público;
- V - um representante indicado pelo Comitê Gestor da Internet no Brasil;
- VI - um representante da sociedade civil;
- VII - um representante da academia; e
- VIII - dois representantes do setor privado.

§ 1º Os representantes serão designados por ato do Ministro de Estado da Justiça e terão mandato de dois anos, permitida uma recondução.

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

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

§ 4º Os representantes referidos nos incisos VI a VIII do **caput** e seus respectivos suplentes serão indicados na forma do regulamento.

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

- I - fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade;
- II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade;
- III - sugerir ações a serem realizadas pelo órgão competente;
- IV - realizar estudos e debates sobre a proteção de dados pessoais e da privacidade; e
- V - disseminar o conhecimento sobre proteção de dados pessoais e privacidade à população em geral.

CAPÍTULO IX  
DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 56. Esta Lei entra em vigor cento e oitenta dias após a data de sua publicação.

Parágrafo único. O órgão competente estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, considerada a complexidade das operações de tratamento e a natureza dos dados.

**Modificação do “caput” do art. 56**, a fim de que seja ampliado o prazo para adequação à nova lei:

*“Art. 56. Esta Lei entra em vigor 36 (trinta e seis) meses após a data de sua publicação.”*

**Justificativa:** tendo em vista as diversas providências necessárias para a devida adequação das empresas à nova legislação, faz-se necessário o alargamento da *vacatio legis*.

Vale ressaltar que o prazo foi sugerido com base naquele estabelecido pela regulação que substituirá a Diretiva 95/46/EC, de 1995 - General Data Protection Regulation (GDPR) -, aprovada recentemente na Europa, que é de 2 anos. No entanto, como no Brasil não há legislação específica nesse sentido, será necessário que a população entenda a relevância da proteção de dados pessoais e as providências que deve adotar para assegurar o seu tratamento, especialmente nos casos em que se requer consentimento, e que as empresas possam investir em tecnologia e implementar procedimentos internos e externos que garantam o adequado cumprimento da lei. Entendemos, assim, que o prazo de 36 meses é o mínimo para que os mais diversos setores da economia possam buscar a sua adequação às novas normas de proteção de dados pessoais para que esta seja de fato efetiva.

**Inclusão do parágrafo primeiro no artigo 56**, passando o atual parágrafo único a constar como parágrafo segundo:

*“Parágrafo Primeiro. Os dados pessoais armazenados pelos responsáveis em conformidade com a legislação vigente à época de sua coleta não estarão sujeitos à obtenção do consentimento dos seus titulares, aplicando-se ao seu tratamento, contudo, as demais disposições desta lei.”*

**Justificativa:** a Lei de Introdução às Normas do Direito Brasileiro ao Código Civil estabelece que a nova lei, ao entrar em vigor, “terá efeito imediato e geral, respeitados o ato jurídico perfeito, a coisa julgada e o direito adquirido”. Ainda, disciplina que o ato jurídico perfeito é aquele “consumado segundo a lei vigente ao tempo em que se efetuou”.

Tal dispositivo é de extrema importância para garantir a segurança jurídica dos atos praticados com base na legislação vigente à época da coleta dos dados pessoais e deve ser aplicado a este projeto, sobretudo no que tange às empresas que exercem, de forma organizada, a atividade de banco de dados. Se diferente for, tais empresas correm o risco de não ter seu principal ativo – o banco de dados – ou sofrerem perda substancial que inviabilize a continuidade de suas atividades após a entrada em vigor da lei.

Cumpra mencionar o exemplo trazido pela doutrinadora Maria Helena Diniz em questão de semelhante relevância, ao dispor que “a alteração da maioria para 18 anos alcançará os jovens que já tiverem atingido essa idade, se se aumentar para 25 anos, respeitará a maioria dos que já tiverem completado 18 anos”.

Nesse sentido, é juridicamente possível entender que os novos requisitos a serem trazidos pela Lei de Proteção de Dados Pessoais não invalidam os dados já colhidos no âmbito da lei anterior, uma vez que os atos já estavam consumados com base na legislação vigente à época da sua coleta. Condiciona-se, porém, novos processamentos, bem como os direitos de acesso e retificação, ao disposto nesta lei.

Caso ainda assim decida-se por desconsiderar o ato jurídico perfeito e determinar que a lei retroaja para alcançar os dados já coletados, sugere-se amparar a previsão do prazo na experiência internacional, prevendo-o já em lei, para conferir segurança jurídica a todos os envolvidos.