UNIVERSIDADE FEDERAL DE JUIZ DE FORA
FACULDADE DE DIREITO
MARIA REGINA DETONI CAVALCANTI RIGOLON

O REGIME JURÍDICO DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS: uma análise da tutela dos dados sensíveis na construção legislativa brasileira

Juiz de Fora
2017

MARIA REGINA DETONI CAVALCANTI RIGOLON

O REGIME JURÍDICO DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS: uma análise da tutela dos dados sensíveis na construção legislativa brasileira

Artigo científico apresentado à Faculdade de Direito da Universidade Federal de Juiz de Fora, como requisito parcial para obtenção do grau de Bacharel. Na área de concentração do Direito Civil, sob orientação do Prof. Dr. Sérgio Marcos Carvalho de Ávila Negri.

Juiz de Fora
2017

FOLHA DE APROVAÇÃO

MARIA REGINA DETONI CAVALCANTI RIGOLON

O REGIME JURÍDICO DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS: uma análise da tutela dos dados sensíveis na construção legislativa brasileira

Artigo científico apresentado à Faculdade de Direito da Universidade Federal de Juiz de Fora, como requisito parcial para obtenção do grau de Bacharel. Na área de concentração do Direito Civil submetida à Banca Examinadora composta pelos membros:

Orientador: Prof. Dr. Sérgio Marcos Carvalho de Ávila Negri
Universidade Federal de Juiz de Fora

Profª. Drª. Kelly Cristine Baião Sampaio
Universidade Federal de Juiz de Fora

Elora Raad Fernandes
Universidade Federal de Juiz de Fora

PARECER DA BANCA

( ) APROVADO

( ) REPROVADO

Juiz de Fora, 23 de novembro de 2017

“Nascer, crescer, morrer, renascer ainda e progredir sempre, tal é a lei”.

Johann Wolfgang von Goethe

RESUMO

A compreensão da proteção dos dados pessoais como direito fundamental autônomo em relação à privacidade demanda a previsão de regime jurídico próprio, ainda inexistente no Brasil, o que enseja variadas iniciativas legislativas com este escopo. Este artigo analisou a consonância dos Projetos de Lei n. 4.060 de 2012 e 5.276 de 2016, que tramitam conjuntamente na Câmara dos Deputados, com um ambiente jurídico adequado à circulação das informações, notadamente com relação aos dados pessoais sensíveis, na medida em que se considera a sua vinculação com a promoção do princípio da dignidade da pessoa humana e com o seu aspecto da liberdade substancial para a construção da personalidade nas sociedades tecnologicamente avançadas. A principal conclusão é de que o Projeto de Lei n. 5.276 de 2016 estabeleceu uma disciplina mais densa de direitos e princípios específicos para a proteção dos dados sensíveis, além de mecanismos de controle, de forma a garantir de modo eficaz a tutela dos dados, apesar de certos institutos merecerem consideração, especialmente com relação ao conceito normativo de dados sensíveis. O tema merece o desenvolvimento de pesquisas e debates, inclusive em outras áreas do conhecimento, com o fim de promover uma moldura jurídica apta a funcionalizar o cenário tecnológico, sobretudo que concerne à proteção de dados, à concretização do princípio da dignidade da pessoa humana.

Palavras-chave: Direitos fundamentais. Dados pessoais. Privacidade. Dignidade.

ABSTRACT

The comprehension of the protection of personal data as an autonomous fundamental right in relation to privacy demands the prediction of its own legal framework, which does not exist in Brazil yet, what leads to various legislative initiatives with this scope. This article examines the consonance of the Bills 4060 of 2012 and 5276 of 2016, which are dealt jointly by the Lower House of the National Congress of Brazil, with an adequate legal framework for the circulation of information, particularly with regard to sensitive personal data, insofar as it is considered to be linked to the promotion of the Principle of Human Dignity and, therefore, with its aspect of substantial liberty for the construction of the personality in technologically advanced societies. The main conclusion is that Bill 5276 of 2016 establishes a more dense regulation of specific rights and principles for the protection of sensitive data, as well as control mechanisms, in a way to ensure effective protection of data, although some institutes deserve consideration, especially with regard to the normative concept of sensitive data. The theme demands the development of research and debates, including in other areas of knowledge, in order to promote a legal framework capable of directing the technological scenario, especially regarding data protection, for the implementation of the Principle of Human Dignity.

Keywords: Fundamental rights. Personal data. Privacy. Dignity.

LISTA DE ABREVIATURAS E SIGLAS

ART.	Artigo
CRFB/88	Constituição da República Federativa do Brasil de 1988
PL	Projeto de Lei

SUMÁRIO

INTRODUÇÃO

A criação de um regime jurídico autônomo para a proteção de dados pessoais é associada à sua compreensão como direito fundamental, na medida em que reconhece-se, com o advento dos avanços tecnológicos, a identificação dos dados com aspectos da personalidade e, portanto, como direito indispensável para a concretização da dignidade humana.

Em sede do ordenamento jurídico brasileiro, todavia, a configuração da proteção de dados como direito autônomo e de matriz fundamental não deriva de uma previsão expressa e literal, mas da consideração dos riscos que o tratamento automatizado traz à personalidade, notadamente em vista das garantias constitucionais da igualdade, liberdade, proteção da intimidade, da vida privada e do objetivo da República consistente na promoção da dignidade da pessoa humana (artigo 1º, III, da Constituição da República Federativa do Brasil de 1988).

A ausência de uma normativa geral acerca da proteção de dados, além de indicar o descompasso do ordenamento jurídico brasileiro com os regimes mais protetivos, como o europeu, evidencia sua importância pela necessidade de funcionalização das situações jurídicas patrimoniais às existenciais em vista da constitucionalização da pessoa, de modo a possibilitar o seu pleno desenvolvimento. Em se tratando dos dados sensíveis, o tema demanda ainda maior consideração.

À luz dessa conjuntura, partiu-se do pressuposto de que a proteção de dados ostenta natureza de direito fundamental e que, destarte, reivindica mecanismos específicos para a sua tutela, motivo pelo qual a pesquisa debruçou-se sobre os Projetos de Lei n. 4.060 de 2012 e 5.276 de 2016 sobre o tema, em trâmite na Câmara dos Deputados, com o fim de averiguar a consonância da pretensa tutela legal dos dados pessoais com a promoção da dignidade humana, sobretudo com o escopo de verificar a existência de disciplina específica dos dados sensíveis.

Buscar-se-á demonstrar que a proteção dos dados sensíveis não pode se desvencilhar da lógica de controle, no âmbito individual e coletivo, e que a sua efetivação está intrinsecamente associada à promoção da dignidade da pessoa humana, não se olvidando que os avanços tecnológicos carecem de construção valorativa, a qual deve se fazer presente também no plano normativo.

Com o paradigma teórico alicerçado no jurista Stefano Rodotá, e mediante emprego da metodologia dedutiva de pesquisa com caráter exploratório, será sustentada a hipótese de que a tutela normativa da pessoa com relação aos seus dados, mormente os sensíveis,

encontra efetividade na medida em que guardar consonância com a disciplina jurídica da circulação das informações proposta pelo autor italiano.

Para tanto, foi efetuada ampla revisão de literatura, com o estudo da evolução do conceito de privacidade até a autonomização do direito à proteção de dados, sua relação com o princípio da dignidade da pessoa, e o desenvolvimento da produção legislativa no contexto internacional. Após este processo, identificou-se o regime jurídico atual da proteção dos dados no Brasil e demonstrou-se como e em qual medida os Projetos de Lei de n. 4.060 de 2012 e 5.276 de 2016 denotam aptidão para a necessária tutela dos dados pessoais, especialmente no que tange ao regime jurídico dos dados sensíveis.

Assim, alcançou-se o objetivo ao qual este trabalho se propôs, qual seja, a investigação do regime jurídico do direito fundamental à proteção de dados pessoais, notadamente dos dados sensíveis nas citadas construções legislativas da Câmara dos Deputados, com a aferição da compatibilidade com a tutela da pessoa, bem como das limitações de determinados institutos, mediante a análise de mecanismos jurídicos para a concretização deste direito fundamental e, por conseguinte, da própria dignidade da pessoa humana inserida na conjuntura tecnológica.

1 DA PRIVACIDADE AO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS

O direito à privacidade pode dizer-se complexo, notadamente porque, como adverte Stefano Rodotá, suportou uma inclusão progressiva de novos aspectos de liberdade em seu conceito, uma vez que as definições não se superaram, exatamente porque baseadas em diferentes requisitos e por operar em níveis diferentes.

Originariamente entendido como “direito de ser deixado só”, segundo definição de Warren e Brandeis (1890, p. 193), relacionada a uma lógica patrimonial e voltada a interesses burgueses, a privacidade progrediu para a acepção de direito à autodeterminação informativa, que inseriu em sua compreensão “o direito de manter o controle sobre as suas próprias informações e de determinar a maneira de construir sua esfera particular”, de forma a assegurar a livre construção da própria esfera privada (RODOTÁ, 2008, pp. 15 e 94).

Maria Celina Bodin de Moraes (2010, p. 136) acrescenta, no contexto das sociedades de informação que estamos inseridos, que a privacidade se manifesta como possibilidade de controlar a circulação das informações e saber quem as usa, o que assume o significado de adquirir um poder sobre si mesmo. A autora salienta tratar-se de uma distinção qualitativa da

autodeterminação informativa, a qual concede a cada um de nós o poder sobre as nossas informações, nossos próprios dados.

A autonomização do direito à proteção de dados para além da tutela da privacidade pode ser percebida no paralelo realizado por Rodotá (2008, p. 27), em sede do qual se distinguia o direito ao respeito à vida privada e familiar como um impedimento à interferência na vida privada de uma pessoa, ao passo que a proteção de dados voltava-se ao estabelecimento de regras sobre mecanismos de processamento de dados e legitimidade para tomada de medidas, as quais não se restringiam aos sujeitos dos dados, porque extensíveis a um órgão público destinado a esta finalidade. Enquanto o primeiro caracterizava-se por uma proteção negativa e estática, a tutela dos dados era dinâmica.

Com efeito, intimamente relacionado à dignidade humana, o direito fundamental à proteção de dados ganhou expressa previsão no ano de 2000 na Carta de Direitos Fundamentais da União Europeia, sendo de valia ressaltar que o documento fez menção em seu art. 3º do "direito à integridade da pessoa", associando à proteção do corpo físico, e no art. 8º prescreveu a proteção de dados, compreendida como a tutela do corpo eletrônico (RODOTÁ, 2008, p. 17).

Em realidade, não se pode olvidar que dados pessoais não são da pessoa, em uma perspectiva puramente patrimonial, mas são a pessoa, como espelho representativo da sua personalidade (DONEDA, 2017), que merece tutela, de plano, com fundamento na cláusula geral inserta no art. 1º, III, da Constituição da República Federativa do Brasil de 1988.[1]

Como consequência, a tutela da integridade da pessoa não deve considerar apenas o corpo que se constitui em uma perspectiva física e em outra eletrônica que se entretecem continuamente: percebe-se, na realidade, um corpo "multiplicado" e "distribuído", que primeiro perdeu sua unidade, a qual foi decomposta em órgãos, células, gametas, depois perdeu sua materialidade, tornando-se uma "senha", com as impressões digitais, DNA, geometria do corpo, entre outros, na esteira de sua acepção eletrônica. A partir desta nova percepção, restou imprescindível reconhecer que a unidade da pessoa somente pode ser reconstituída com a extensão ao corpo eletrônico de garantias elaboradas para o corpo físico (RODOTÁ, 2004, pp. 103-104).

---

[1] "L'elettronica induce a concludere che 'Noi siamo le nostre informazioni'", sintetizou Rodotá na sua obra *Dal sogetto alla persona*, oportunidade em que também advertiu para uma interpretação literal da assertiva, sobretudo frisando tratar-se de uma crítica a esta tendência. Perceber a lição do autor ressalta senão a necessidade de cautela com os dados pessoais, na medida em que a tecnologia tem aptidão para ampliar ou reduzir o conceito de pessoa, como ensina o jurista. (RODOTÁ, 2007, p. 53 apud SCHULMAN, 2016, p. 330-360).

Considerando a presença do corpo eletrônico na conjuntura tecnológica em que estamos situados, percebe Stefano Rodotá (2008, p. 241) que a simples disponibilidade de uma tecnologia não legitima todas as suas utilizações, de modo que estas devem ser avaliadas com valores distintos daqueles fornecidos pela própria tecnologia. Aduz o jurista que "a privacidade não é um obstáculo, porém a via pela qual as inovações científicas e tecnológicas possam legitimamente entrar nas nossas sociedades e nas nossas vidas".

Destarte, a atenção deve se voltar para a "constitucionalização da pessoa", o que, no cenário da tecnologia contemporâneo, não desconsiderando a sua perspectiva futura por ora imensurável e partindo da premissa de que as situações patrimoniais devem ser funcionalizadas às existenciais (TEPEDINO, 2009, pp. 3-4),[2] não prescinde da efetiva tutela dos dados pessoais. Como percebe Rodotá (2015, p. 1), "a palavra *privacy* evoca não apenas uma necessidade de intimidade, mas sintetiza as liberdades que nos pertencem no mundo novo onde vivemos".

Deveras, a compreensão e o governo das transformações determinadas pelos avanços tecnológicos apenas é viável se guardar sintonia com instrumentos prospectivos aptos a redefinir os princípios fundadores das liberdades individuais e coletivas sob os paradigmas dos novos tempos (RODOTÁ, 2015, p. 8). Em realidade, com o imperativo da constitucionalização da pessoa, nem tudo que é tecnicamente possível é socialmente desejável, eticamente aceitável e juridicamente admissível (RODOTÁ, 2004, p. 101).

2 A CONCRETIZAÇÃO DA DIGNIDADE HUMANA NO ÂMBITO DA PROTEÇÃO DOS DADOS PESSOAIS SENSÍVEIS

Com relativização da *summa divisio* entre o Direito Público e o Privado, duas circunstâncias históricas alteraram radicalmente a preocupação da doutrina nas últimas décadas, quais sejam, a dignidade da pessoa humana alçada a paradigma axiológico das relações privadas e as novas tecnologias, as quais reformularam o conteúdo da autonomia privada (TEPEDINO, 2016, p. 20).

Na perspectiva civil-constitucional, o direito privado, sob a égide da irradiação dos princípios constitucionais nos espaços de liberdade individual, é o que a ordem pública

[2] Com efeito, acrescente-se que uma das premissas metodológicas da constitucionalização do Direito Civil consiste na preeminência das situações existenciais sobre as patrimoniais. Tendo em vista a superioridade normativa da Constituição e, dentro dela, a centralidade do princípio da dignidade da pessoa humana, impõe-se a releitura de todos os institutos de Direito Civil, reconhecendo que nosso ordenamento fez uma escolha no sentido de privilegiar o "ser" sobre o "ter". (KONDER, Carlos Nelson. Vulnerabilidade patrimonial e vulnerabilidade existencial: por um sistema diferenciador. *Revista de Direito do Consumidor*, v. 99, p. 107, 2015).

constitucional permite que possa sê-lo, como destaca Gustavo Tepedino (2009, p. 3). Partindo deste pressuposto, o regime jurídico dos dados pessoais, sobretudo dos sensíveis, deve ser funcionalizado às situações existenciais e, portanto, à dignidade da pessoa que, compreendida como valor e princípio, compõe-se dos princípios da liberdade privada, da integridade psicofísica, da igualdade substancial (art. 3º, III, da CRFB/88) e da solidariedade social (art. 3º, I, da CRFB/88).[3]

Em realidade, o exercício das liberdades individuais, como componente da dignidade da pessoa, estabelece relação intrínseca de dependência com a tutela dos dados pessoais,[4] especialmente dos sensíveis, que são aqueles associados às opções basilares da *persona* e, portanto, aptos a gerar situações de discriminação e desigualdade.[5] Como ressalta Baião e Gonçalves (2017, p. 5), "enquanto parte essencial da pessoa humana, a dignidade é autorreferente e condição intrínseca da liberdade, pois não existe dignidade sem autonomia".

Portanto, o âmbito propício ao pleno desenvolvimento da personalidade demanda que seja assegurada a maior autonomia possível, conferindo à pessoa a faculdade de rever e construir sua identidade, fora de uma lógica cristalizada (BAIÃO E GONÇALVES, 2017, p. 8), uma vez que "a autonomia é elemento ético da dignidade", como destaca Luís Roberto Barroso (2010, p. 24).

Outrossim, a proteção dos dados pessoais ganha ainda maior relevo ao se vislumbrar a lógica do mercado, na qual a fragmentação da pessoa em dados potencializa uma nova versão da abstração da pessoa, que usualmente passa a se traduzir em matéria prima, na forma de dados, em produto, porque comercializável, e em destinatário na cadeia de consumo, em face da paradoxal hiperpessoalização com base nos dados coletados (SCHULMAN, 2016, pp. 336-345).

---

[3] Ainda com a lição de Maria Celina Bodin de Moraes, é de se ressaltar que "o substrato material da dignidade assim entendida pode ser desdobrado em quatro postulados: i) o sujeito moral (ético) reconhece a existência dos outros como sujeitos iguais a ele, ii) merecedores do mesmo respeito à integridade psicofísica de que é titular; iii) é dotado de vontade livre, de autodeterminação; iv) é parte do grupo social, em relação ao qual tem a garantia de não vir a ser marginalizado. São corolários desta elaboração os princípios jurídicos da igualdade, da integridade física e moral – psicofísica –, da liberdade e da solidariedade" (*Danos à pessoa humana, uma leitura civil-constitucional dos danos morais*, Rio de Janeiro: Renovar, 2003, p. 85).

[4] Danilo Doneda acentua a distinção entre os termos "dado" e "informação", destacando o primeiro com uma conotação primitiva, como uma informação em estado potencial, antes de ser transmitida, ao passo que a informação alude a algo além da representação contida no dado, chegando ao limiar da cognição. Aduz o autor, ainda, que a informação pode se associar a valores distintos, como a própria liberdade de informação. (DONEDA, Danilo. *A proteção dos dados pessoais como um direito fundamental*. Espaço Jurídico, Joaçaba, v. 12, n. 2, p.91-108, jul/dez 2011. Disponível em: <http://editora.unoesc.edu.br/index.php/espacojuridico/article/download/1315/658>. Acesso em: 01 set. 2017, p. 93-94).

[5] Neste sentido destaca Maria Celina Bodin de Moraes ao prefaciar a obra "A vida na sociedade de vigilância" de Stefano Rodotá. RODOTÀ, Stefano. *A vida na sociedade da vigilância*, cit., p. 10.

Como aponta Rodotá (2004, pp. 93-100 e 103), as contradições são evidentes, na medida em que a fragmentação da pessoa reduzida a dados pessoais é mecanismo utilizado tanto para atividades ilegais, quanto para a proteção e promoção da pessoa, como no emprego de dados biométricos e genéticos.[6]

Com tais considerações, emerge que pela defesa da pessoa e de seu corpo, defendem-se valores fundamentais dos sistemas democráticos, máxime a dignidade humana, os quais não podem ser limitados ou sacrificados sem gerar consequências que podem se abeirar de sistemas totalitários (RODOTÁ, 2004, p. 97), incompatíveis com o pleno desenvolvimento da personalidade.

3 EVOLUÇÃO LEGISLATIVA DA PROTEÇÃO DE DADOS

Com o fim verificar quais os elementos que se coadunam com sistemas normativos avançados na tutela de dados, não se prescinde de uma análise histórica da produção legislativa pertinente no cenário internacional.

Destarte, vale evidenciar a classificação evolutiva dessas leis realizada por Viktor Mayer-Scönberger (1997, p. 223-224, apud DONEDA, 2011, p. 96-98), sintetizada em quatro gerações, desde uma noção mais técnica e restrita a uma concepção ampla, condizente com a profundidade dos avanços tecnológicos e com o objeto da tutela, na condição de direito fundamental autônomo.

A primeira geração das leis de proteção de dados voltava-se a regular centros elaboradores de dados que concentrariam a coleta e a gestão de informações pessoais, normatizando a concessão de autorizações para a criação desses bancos e a posterior fiscalização pelos órgãos públicos. Registre-se que o Estado era vislumbrado como controlador e principal usuário de tais dados, bem como destinatário das respectivas normas. Com relação à estrutura tecnocrática das normas, destacavam-se princípios demasiado abstratos, voltados à tutela dos bancos de dados, e não à privacidade em si, e sem previsão da participação do cidadão.

Com a multiplicação dos centros de processamento de dados adveio a segunda geração, ao final da década de 1970, direcionada à consideração da personalidade e dos dados

[6] Nesta seara, adverte Rodotá que o amplo espectro de possibilidades de utilização dos dados genéticos, essencialmente dotado de natureza sensível, explica os motivos pelos quais vêm se multiplicando as propostas tendentes a efetuar o tratamento desses dados para diversas finalidades. Não se pode olvidar, todavia, as preocupações relativas ao risco de discriminações e de limitações das liberdades civis e políticas que a constituição de bancos de dados neste sentido pode promover, especialmente no que concerne aos dados sensíveis. (RODOTÁ, Stefano. Transformações do corpo. *Revista Trimestral de Direito Civil*, v. 19, p. 91-107, pp. 93-100 e 103).

pessoais como uma liberdade negativa a ser exercida pelo indivíduo, com o seu núcleo não mais situado apenas no fenômeno computacional. Começaram a surgir, ainda incipientes, instrumentos individuais de controle facultados à pessoa.

O aumento dos avanços tecnológicos não tardaram, e na medida em que se percebeu que o fornecimento de dados pessoais pelos cidadãos havia se tornado um requisito essencial para a sua participação na vida social, abriu-se margem a uma terceira geração de leis, na década de 1980, que teve por fim abranger além de uma liberdade de fornecer ou não os próprios dados pessoais, mas a garantia efetiva de seu livre exercício. Para tanto, estabeleceram-se meios de proteção dos dados em situações em que existiam condicionamentos na livre decisão da pessoa e buscou-se inserir o titular nas fases sucessivas de tratamento, além de prever garantias como o dever de informação.

Verificado que a autodeterminação informativa era privilégio de uma minoria que conseguia arcar com os custos econômicos e sociais de seu exercício, promoveu-se a quarta geração de leis, voltada a suprir as defasagens da perspectiva individualista existente até então. Assim, sob a premissa de que a tutela dos dados pessoais não poderia estar adstrita a uma escolha individual, considerou-se necessário elevar a sua proteção a um padrão coletivo.

De plano, reconheceu-se o patente desequilíbrio nas relações entre as entidades coletoras de dados e os titulares, de modo que o mero reconhecimento do direito à autodeterminação informativa no âmbito formal não era suficiente. Assim sendo, paradoxalmente, buscou-se reduzir o papel da decisão individual do titular, uma vez reconhecida que a proteção de certos dados deveria se dar em seu maior grau, como no caso dos dados sensíveis.

Igualmente podem ser destacadas como características dessa quarta geração a disseminação do modelo das autoridades independentes para a atuação da lei, associado à noção de *enforcement*, e a criação de normativas específicas para a proteção de dados.[7]

Durante essa evolução normativa, a matéria de proteção de dados pessoais associou-se a uma disciplina jurídica de princípios que constituíram, no dizer de Danilo Doneda (2011, p. 101), a "espinha dorsal" de diversas leis, tratados, convenções e acordos entre instituições privadas, a saber, os princípios da publicidade, da exatidão, da finalidade, do livre acesso e da segurança física e lógica. Conhecidos como *Fair Information Principles*, podem ser sintetizados da seguinte forma:

---

[7] O modelo identificado pela quarta geração é representado pelos países europeus que adotaram as Diretivas europeias sobre proteção de dados, como a Diretiva 95/46/CE e a Diretiva 2000/58/CE. (DONEDA, Danilo. *A proteção dos dados pessoais como um direito fundamental*, cit., p. 102).

a) Princípio da publicidade (ou da transparência), segundo o qual a existência de um banco de dados deve ser de conhecimento público, seja através da necessidade de autorização prévia para funcionar, da notificação a uma autoridade da sua existência, ou do envio de relatórios periódicos;

b) Princípio da exatidão: os dados armazenados devem ter correspondência com a realidade, de forma que a coleta e tratamento devem se dar com cuidado e correção, atentando-se para a necessidade de atualizações periódicas;

c) Princípio da finalidade: a utilização dos dados deve se dar nos limites da finalidade informada ao interessado antes da coleta. Doneda (2011, p. 100) alerta para a relevância prática deste princípio, porquanto com base nele fundamenta-se a restrição de transferência de dados pessoais a terceiros, além de que a partir dele pode estruturar-se um critério para valorar a razoabilidade da utilização de certos dados para determinado fim;

d) Princípio do livre acesso: o indivíduo deve ter acesso ao banco de dados no qual suas informações estão armazenadas, o que inclui o direito à obtenção de cópias desses registros e ao controle desses dados. Conciliado com o princípio da exatidão, o particular também poderá corrigir informações incorretas, suprimir aquelas obsoletas ou imperfeitas e proceder a acréscimos;

e) Princípio da segurança física e lógica: os dados devem ser protegidos contra os riscos que impliquem em seu extravio, destruição, modificação, transmissão ou acesso não autorizado.

Não obstante, igualmente ao avaliar a experiência passada, Rodotá (2008, pp. 87-88) considerou que a rápida obsolescência das disciplinas muito rígidas indica para a necessidade de adoção de intervenções institucionais dotadas de maior flexibilidade e, destarte, elaborou as premissas necessárias para um ambiente jurídico favorável a uma disciplina adequada da circulação das informações. As premissas são as seguintes:

a) Uma disciplina legislativa de base que se constitua essencialmente por cláusulas gerais e normas processuais;

b) Normas voltadas a casos específicos, possivelmente previstas em leis autônomas, referentes a atividades de determinados sujeitos ou com a disciplina de categorias específicas de informações;

c) Uma autoridade administrativa independente, que eventualmente titularize poderes para adaptar a situações particulares os princípios previstos nas cláusulas gerais;

d) Previsão de uma disciplina de recurso à autoridade judiciária, não apenas nos sistemas nos quais tal se depreende de exigência constitucional, mas de modo geral, com o fim de enraizar nesta seara princípios análogos aos de um *Bill of Rights* ou do *Due Process*, no caminho de uma linha tendente a aproximar a matéria estudada dos direitos civis;

e) Previsão de um controle difuso pela iniciativa de grupos e cidadãos.

Com fundamento na esposada construção de Stefano Rodotá, mister citar a presente conjuntura normativa da proteção de dados no Brasil, para então adentrar aos Projetos de Leis selecionados em trâmite no Congresso Nacional.

4 O REGIME JURÍDICO ATUAL DA PROTEÇÃO DE DADOS NO BRASIL

A tutela dos dados pessoais na América do Sul é marcadamente inspirada pela normativa da União Europeia, em razão de laços históricos e culturais que se estendem para o campo legal e institucional. Todavia, a despeito de ser a maior economia da região, o Brasil não possui uma lei geral sobre a proteção de dados pessoais (VIOLA et. al., 2016, p. 362).

A ordem jurídica pátria disciplina, contudo, pontualmente os dados da pessoa. Iniciando com a Constituição da República Federativa do Brasil de 1988, os dados, até mesmo sob a perspectiva da privacidade, encontram residência nos incisos X e XII do art. 5º, sendo de registrar o remédio judicial do *habeas data*, previsto no inciso LXXII do citado dispositivo.

Em sede infraconstitucional, o Código Civil incluiu o direito à privacidade no rol dos direitos da personalidade em seu art. 21, e leis como o Código de Defesa do Consumidor (Lei n. 8.078/1990), a Lei do Cadastro Positivo (Lei n. 12.414/2011), a Lei de Acesso à Informação (Lei n. 12.527/2011), o Marco Civil da Internet (Lei n. 12.965/2014) e a própria legislação do *habeas data* (Lei n. 9.507/97) também disciplinaram incidentalmente a matéria de dados.

Neste tocante, é de se ressaltar que o Marco Civil da Internet, ao elencar os princípios da disciplina da rede virtual no Brasil, destacou a proteção dos dados pessoais, a se dar na forma da lei, a qual ainda não foi promulgada. Não é demais anotar que a tutela dos dados usurpa o âmbito da internet, o que evidencia a ausência de um regulamento geral da disciplina.

Lado outro, vale destacar a existência de menção à natureza de direito fundamental autônomo da proteção de dados pessoais na Declaração de Santa Cruz de La Sierra, documento final da XIII Cumbre Ibero-Americana de Chefes de Estado e de Governo, firmada pelo Governo Brasileiro em 15 de novembro de 2003, como se destaca de seu item 45:

> Estamos também conscientes de que a proteção de dados pessoais é um direito fundamental das pessoas e destacamos a importância das iniciativas reguladoras ibero-americanas para proteger a privacidade dos cidadãos, contidas na Declaração de Antigua, pela qual se cria a Rede Ibero-Americana de Protecção de Dados, aberta a todos os países de nossa Comunidade.

Ante a lacuna jurídica identificada, considerando que o estabelecimento de uma disciplina jurídica geral de dados, máxime dos dados sensíveis, se apresenta, na conjuntura hodierna das sociedades de informação, como indispensável à constitucionalização da pessoa, procedeu-se à análise dos Projetos de Lei em trâmite na Câmara dos Deputados de n. 4.060 de 2012 e 5.276 de 2016.

5 A TUTELA DOS DADOS SENSÍVEIS NOS PROJETOS DE LEI N. 4.060 DE 2012 E 5.276 DE 2016

A construção de um regime jurídico próprio para a proteção de dados fundamenta no Brasil a existência de projetos de lei em trâmite no Congresso Nacional,[8] tendo sido escolhidos para o presente estudo os de n. 4.060 de 2012 e 5.276 de 2016, que seguem em apenso no processo legislativo e, portanto, devem ser avaliados de forma conjunta em seus aspectos mais incisivos acerca da tutela dos dados sensíveis.

5.1 Justificativas das iniciativas legais

Com o escopo de justificar o Projeto de Lei n. 4.060/2012 sobre o tratamento de dados pessoais, indicou-se na iniciativa parlamentar que "se faz necessário estabelecer normas legais para disciplinar tais relações, especialmente para dar proteção à individualidade e a privacidade das pessoas, sem impedir a livre iniciativa comercial e de comunicação" (BRASIL, 2012, p. 7).

[8] Vale destacar a existência de três Projetos de Lei em trâmite no Senado Federal que seguem apensados, quais sejam, PL 330 de 2013, que dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências; PL 131 de 2014 que dispõe sobre o fornecimento de dados de cidadãos ou empresas brasileiros a organismos estrangeiros e o PL 181 de 2014 que estabelece princípios, garantias, direitos e obrigações referentes à proteção de dados pessoais.

Por seu turno, na justificativa do Projeto de Lei n. 5.276/2016, que dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural, registrou-se a forte influência internacional na iniciativa, sobretudo com relação à Resolução da Organização das Nações Unidas de 25 de novembro de 2013 sobre "Direito à Privacidade na Era Digital".[9]

Outrossim, ao ressaltar a assimetria de poder dos indivíduos e os responsáveis pelas operações de tratamento de dados, foi destacada a necessidade da sua utilização legítima, com estabelecimento de mecanismos específicos, com as funções de proteger o titular dos dados e favorecer a sua utilização dentro de um patamar de segurança, transparência e boa-fé. Deveras, conceituou-se o PL 5.276/2016 como:

> Arquitetura regulatória capaz de fazer emergir o tema da proteção de dados pessoais como um verdadeiro vetor de políticas públicas, composto por instrumentos estatutários, sancionatórios, bem como por um órgão administrativo, responsável pela implementação e aplicação da legislação (BRASIL, 2016, p. 22).

5.2 O conceito normativo dos dados sensíveis

Ambos os projetos de lei disciplinam de forma específica a tutela dos dados sensíveis, destacando-os dos demais dados pessoais e, por conseguinte, prescrevendo normativa própria.

A começar pela definição, o PL 4.060/ 2012 estabelece no art. 7º, inciso IV, que os dados sensíveis são "informações relativas à origem social e étnica, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas do titular", ao passo que o PL 5.276/2016 prescreve em seu art. 5º, inciso III, os dados sensíveis como "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".

Desponta de modo evidente que o PL 5.276/2016 apresenta um rol mais amplo que o PL 4.060/2012, porquanto atribui a natureza de dado sensível à filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, às informações relativas à saúde e aos

[9] A citada Resolução da ONU associou-se diretamente ao episódio em que Edward Snowden, ex-técnico da CIA, vazou informações sigilosas de segurança dos Estados Unidos, as quais revelaram em detalhes alguns dos programas de vigilância que o país usa para espionar a população americana - utilizando servidores de empresas como Google, Apple e Facebook – e vários países da Europa e América Latina, entre eles o Brasil, inclusive com monitoramento da então presidente Dilma Rousseff em conversas com seus assessores. (G1. Entenda o caso de Edward Snowden, que revelou espionagem dos EUA. *G1*. São Paulo. 02 jul. 2013. Disponível em: <http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>. Acesso em: 15 set. 2017).

dados biométricos. Por sua vez, o PL 4.060/2012 estabeleceu a distinção com relação à origem social da pessoa, o que não foi abordado no outro projeto.

Ao partir para uma comparação com a Convenção do Conselho da Europa n. 108, "Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automático de Dados Pessoais", precisamente com o seu art. 6º,[10] verifica-se que a despeito de apresentar um rol mais conciso do que seriam os dados sensíveis, ressaltou a tutela dos dados pessoais relativos a condenações criminais, que detêm caráter marcadamente sensível.

Como bem apontado por Maria Celina Bodin de Moraes[11], dados sensíveis podem ser compreendidos como aqueles que têm aptidão para gerar situações de discriminação e desigualdade, podendo-se inferir a dificuldade de prever um rol taxativo de quais as situações que se enquadram neste conceito.

Destarte, emerge que a tutela deveria se dar mediante uma cláusula geral capaz de englobar todos esses casos, valendo-se da orientação de Rodotá no sentido de que a disciplina legislativa de base adequada deveria se constituir essencialmente de cláusulas gerais, justamente com o fim de oxigenar a legislação, o que não se verificou no cenário em tela.

Ademais, no tangente às inúmeras situações que têm o condão de caracterizar práticas discriminatórias alheias à promoção da pessoa no Estado Democrático de Direito, não se pode olvidar dos perigos de uma homogeneização dos indivíduos no que concerne aos dados sensíveis, categorizando-os e inserindo-os em padrões de "certo" ou "errado".

5.3 O regime jurídico principiológico

É cediço que a normatização por princípios e por cláusulas gerais estabelece salutar caráter de flexibilidade nos diplomas jurídicos, na medida em que autoriza uma adaptação a diferentes conjunturas com o fim de proporcionar uma tutela efetiva e consentânea com os anseios sociais. Neste sentido indica Rodotá para o estabelecimento de cláusulas gerais, mormente em se tratando dos exponenciais avanços tecnológicos nesta seara: "adverte-se desta forma para a necessidade de individualizar princípios, de associá-los a tendências de longo prazo" (RODOTÁ, 2008, p. 42).

---

[10] O artigo 6º dispõe que "Dados pessoais que revelem a origem racial, opiniões políticas, religiosas ou de outras crenças, bem como dados relativos à saúde pessoal ou à vida sexual não podem ser processados automaticamente ao menos que leis nacionais estabeleçam garantias adequadas. O mesmo se aplica a dados pessoais relativos a condenações criminais." (CONSELHO DA EUROPA. *Convenção Para A Protecção das Pessoas Relativamente Ao Tratamento Automatizado de Dados de Carácter Pessoal*. Disponível em: <https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm>. Acesso em: 10 set. 2017).

[11] É a lição de Maria Celina Bodin de Moraes no prefácio de "A vida na sociedade da vigilância". RODOTÀ, Stefano. *A vida na sociedade da vigilância.* A privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 10.

Isso posto, é de se atentar que o PL 5.275/2016 disciplinou em seu art. 6º a necessidade de observância da boa-fé e dos princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção e não discriminação, os quais se identificam, a despeito da nomenclatura distinta em certos casos, e inclusive vão além dos *Fair Information Principles.*

Como consectário dessa principiologia, o art. 18 do citado projeto dispõe sobre um rol de direitos atribuídos aos titulares dos dados pessoais, como mecanismos concretos para efetivar as normas dotadas de maior abstração.[12]

Por seu turno, o PL 4.060/2012 adstringiu seu regime jurídico principiológico, consoante seu art. 5º, aos "princípios constitucionais da Defesa do Consumidor, Livre iniciativa, Liberdade de Comunicação e Ordem Econômica, nos termos dos artigos 1º, IV, 5º, inc. IX, XXXII, 170 e 220 da Constituição Federal", o que se apresenta como limitado frente à normativa inserta no outro projeto, além de não se vincular a princípios específicos para a tutela dos dados.

5.4 Segurança pública e proteção de dados

O PL 5.276/2016 excluiu expressamente de seu âmbito de incidência o tratamento de dados realizado para fins exclusivos de segurança pública, de defesa nacional, de segurança do Estado ou de atividades de investigação e repressão de infrações penais, conforme se extrai de seu art. 4º, III, relegando tal incumbência à legislação específica, conforme o parágrafo 1º do mesmo dispositivo. Neste tocante, destaque-se que os dados associados a estas finalidades são frequentemente dotados de natureza sensível.[13]

---

[12] O art. 18 dispõe que: "O titular dos dados pessoais tem direito a obter, em relação a 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. (...)" (BRASIL. Projeto de Lei n. 5.276, de 13 de maio de 2016 da Câmara dos Deputados. Brasília, Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1457459&filename=PL+5276/2016>. Acesso em: 10 set. 2017).

[13] É emblemático o caso de Truro, Massachussets, nos Estados Unidos, em que foram realizadas testagens em massa em janeiro de 2005, por motivo do assassinato de uma mulher, Christa Worthington, ocorrido três anos antes. Setecentos e noventa homens foram chamados a ceder saliva, compreendida como fragmentos de DNA, de forma a permitir a comparação com o material genético colhido na cena do crime. O sargento David Perry, da Polícia de Truro, asseverou que o programa é voluntário, mas que especial atenção seria dada àqueles que se recusarem a cooperar, acrescentando que eles estavam em busca de quem tinha algo a esconder. (BELLUCK, Pam. To Try to Net Killer, Police Ask a Small Town's Men for DNA. *New York Times.* Boston. 10 jan. 2005.

Valendo-se da premissa elencada por Rodotá no sentido de que é necessário a um ambiente jurídico favorável à tutela das informações o estabelecimento de normas específicas, referentes a atividades de determinados sujeitos ou com a disciplina de categorias específicas de informações, é de se identificar uma consonância com a previsão indicada, porquanto atribuiu à legislação específica a tutela dos dados pessoais nos casos afetos à segurança pública *lato sensu*, sujeitando-a aos princípios gerais estabelecidos no PL 5.276/2016.[14]

Ademais, nos parágrafos 2º e 3º, do art. 4º, do PL 5.276/2016, é registrada a competência exclusiva das pessoas jurídicas de direito público neste âmbito, exceto em procedimentos realizados por pessoas jurídicas de direito privado sob a supervisão daquelas, devidamente informado ao órgão de controle competente, bem como a possibilidade dos mesmos órgãos solicitarem aos responsáveis relatórios de impacto de privacidade.

No que tange ao PL 4.060/2012, é de se atentar para a previsão que exclui da abrangência da lei o tratamento de dados referentes aos bancos de dados utilizados para a pesquisa de administração pública, investigação criminal ou inteligência, conforme seu art. 6º, III, sem fazer qualquer menção à necessidade de legislação específica para tal mister, o que acaba por ser perigoso, notadamente por relegar um vácuo legal à matéria. Não bastasse, ao contrário do que se dá no outro projeto, não se estabelece qualquer vinculação aos princípios gerais de proteção de dados, a fazer emergir considerável incompatibilidade com a tutela da pessoa.

Em realidade, como acentua Rodotá (2004, p. 95), os valores de segurança e proteção de dados não são incompatíveis e podem ser ponderados. No entanto, a supressão da tutela dos dados deve ser excluída quando acarreta violação da dignidade da pessoa humana, referência inviolável, seja inspirando-se na Carta dos Direitos Fundamentais da União Europeia, seja com fulcro na Constituição da República de 1988, o que deve ser considerado na respectiva legislação específica, máxime em vista da constitucionalização da pessoa.

5.5 O consentimento e o tratamento de dados

A disciplina específica dos dados sensíveis também abarca o instituto do consentimento, impondo-se proceder, de plano, à sua análise no âmbito geral dos dados pessoais.

Disponível em: <http://www.nytimes.com/2005/01/10/us/to-try-to-net-killer-police-ask-a-small-towns-men-for-dna.html>. Acesso em: 09 set. 2017).

[14] Na justificativa do PL 5.276/2016 foi indicado que a apresentação do projeto de lei referente à segurança pública se daria posteriormente ao já apresentado (BRASIL. Projeto de Lei n. 5.276, de 13 de maio de 2016 da Câmara dos Deputados, cit., p. 21).

Ao elencar as hipóteses em que o tratamento de dados pessoais poderá se dar, merece destaque o art. 7º, I, do PL 5.276/2016, segundo o qual demanda-se o "consentimento livre, informado e inequívoco". Aduz o art. 9º do referido projeto que tal consentimento deverá se dar por escrito ou por qualquer outro meio que o certifique, regulamentando em seus parágrafos mecanismos para assegurar o seu livre exercício, bem como a possibilidade de revogação a qualquer momento, mediante manifestação expressa do titular.

Por sua vez, o PL 4.060/2012 não estabelece um rol de hipóteses em que será permitido o tratamento dos dados pessoais, apenas discriminando de forma genérica que tal deverá se dar com "lealdade e boa fé, de modo a atender aos legítimos interesses dos seus titulares" em seu art. 9º, inexistindo menção à necessidade do consentimento, o que se revela dissonante noção de autodeterminação informativa. No entanto, é assegurado em seu art. 13 o direito ao bloqueio do registro, salvo se necessário para cumprimento de obrigação legal ou contratual.

Em se tratando dos dados sensíveis, todavia, a normativa é diversa. No PL 5.276/2016, o tratamento de dados sensíveis é vedado, excetuando-se as hipóteses discriminadas no art. 11. Outrossim, a disciplina jurídica dos dados sensíveis neste tocante é estendida aos dados pessoais que tenham o condão de revelar dados sensíveis, como dispõe o parágrafo 1º, do art. 11, acrescentando o parágrafo 2º que o tratamento dos dados sensíveis não poderá ser realizado em detrimento do seu titular.

No inciso I do art. 11, o permissivo legal é no sentido de que o tratamento dos dados sensíveis poderá se dar com o consentimento livre, inequívoco, informado, expresso e específico, a ser fornecido pelo titular mediante manifestação própria, distinta da manifestação do consentimento relativa a outros dados pessoais e com informação prévia e específica sobre a natureza dos dados a serem tratados, com alerta dos riscos envolvidos no seu tratamento.

A despeito de parecerem adequadas as medidas eleitas pelo legislador para a tutela do consentimento, convém destacar a advertência de Rodotá (2004, p. 103) no sentido de que jamais deve ser permitido ultrapassar a proibição de utilizações específicas de dados pessoais, ainda que com o consentimento dos interessados, uma vez considerado que este consenso pode estar condicionado por diversos fatores e parece, de qualquer modo, inadequado para resolver problemas que dizem respeito a aspectos essenciais da personalidade, mormente no que toca aos dados sensíveis. Igualmente, não se pode olvidar da figura do "contratante vulnerável", caracterizado justamente pela ausência de liberdade substancial, uma vez considerada a assimetria de poder dos sujeitos envolvidos (RODOTÁ, 2008, p. 138).

Com o objetivo de minimizar essa diferença de poder, pode-se salientar a previsão do art. 8º, VII, "a" do, PL 5.276/2016, segundo a qual é garantido ao titular a possibilidade de não fornecer o consentimento, na hipótese em que esse é requerido, mediante o fornecimento de informações sob as consequências da negativa, bem como o parágrafo 4º, também do art. 8º, que estabelece que quando o consentimento for condição para a concessão de produto, serviço ou exercício de direito, o titular deverá ser informado com destaque sobre tal fato e sobre os meios pelos quais poderá exercer o controle sobre o tratamento de seus dados. Como normativa geral e eminentemente protetiva, deve se estender aos dados sensíveis.

Ademais, volvendo ao art. 11, seu parágrafo 2º que estabelece a impossibilidade do tratamento dos dados sensíveis em desfavor do titular merece destaque e deve ser interpretado de forma ampla, como verdadeira cláusula geral, no sentido de que ainda que munido do consentimento do titular, o responsável pelo tratamento de dados não poderá fazê-lo se tal significar prejuízo ao interessado. Destaque-se que a ressalva do dispositivo referente à possibilidade de prejuízo ao titular se previsto em legislação específica demanda atenção, mormente porque se dá em termos genéricos, bem como não se pode olvidar da prevalência na ordem jurídica nacional da dignidade da pessoa.

Noutro giro, o art. 11 dispõe em seu inciso II as hipóteses em que será dispensado o consentimento do titular para o tratamento dos dados sensíveis, demandando uma análise pormenorizada as alíneas "b" e "c" que prescrevem, respectivamente, a dispensa para o "tratamento e uso compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos" e "realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis".

De plano, parece razoável que a previsão da anonimização dos dados sensíveis se estenda também à hipótese da alínea "b", posto que a finalidade eminentemente pública não retira a necessária preservação do titular.

No tangente à alínea "c", o parágrafo 3º, do art. 11 ressalva que ela não se aplicará caso as atividades de pesquisa estejam vinculadas a atividade comercial, de administração pública, quando a pesquisa não for a atividade principal ou a legalmente estabelecida do órgão, ou quando for relativa à investigação criminal ou inteligência, de modo que pela técnica legislativa adotada é razoável compreender que o consentimento será exigido, em vista da sua finalidade, a exemplo das atividades de mercado, e da tutela bens jurídicos correlatos, como no caso da investigação criminal. Nesta esteira, o parágrafo 4º estabelece

que nas citadas hipóteses, sempre que possível, será assegurada a anonimização dos dados pessoais.

Ademais, deve ser evidenciada a alínea "f" do inciso II, art. 11, a qual versa sobre a dispensa do consentimento quando a utilização dos dados sensíveis for indispensável para a tutela da saúde, com procedimento realizado por profissionais da área ou por entidades sanitárias.

Tal hipótese pode ser perigosa ou deve, minimamente, ser interpretada no estrito interesse do particular, notadamente porque, a despeito da dispensa do consentimento neste caso, ao versar sobre a sua concessão, Rodotá (2008, p. 138) adverte que em sendo a cessão de dados afetos à saúde condição para a concessão de um serviço, especialmente nas práticas mercadológicas, ou como necessário à própria possibilidade da cura, a tutela da privacidade deveria se dar por dois meios, a saber, estímulo à cobertura pública das despesas médicas ou tornando indisponíveis as informações sobre a saúde, partindo da premissa de que a saúde é um direito fundamental, que abrange aspectos particularmente delicados da personalidade.

Em outro âmbito do anteprojeto, registre-se que é assegurado ao titular a possibilidade de se opor ao tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, caso verificado o descumprimento da lei, nos termos do parágrafo 1º, do art. 18, do PL 5.276/2016, o que emerge como mecanismo de controle facultado ao particular.

Com relação ao PL 4.060/2012, identifica-se a adoção de técnica legislativa diversa, uma vez que é admitido o tratamento dos dados sensíveis mediante autorização do titular, quando não for por ele solicitado, por qualquer meio que permita a manifestação da sua vontade, a evidenciar a adoção de critério bem menos exigente e propício à concretização do consentimento livre e informado, portanto, aquém da disciplina estabelecida no outro projeto. Outrossim, dispensa-se o consentimento quando houver imposição legal, sem discriminar, contudo, as hipóteses de incidência.

5.6 Compartilhamento de dados

Em matéria de transferência de dados, é de se atentar para a incidência do princípio da finalidade, o qual dispõe que a utilização dos dados deve se dar nos limites da finalidade informada ao interessado antes da coleta, de forma que com base nele fundamenta-se a restrição do compartilhamento de dados pessoais a terceiros, além de que a partir dele pode estruturar-se um critério para valorar a razoabilidade da utilização de certos dados para determinado fim, como ensina Doneda (2011, p. 100).

A aplicação do princípio da finalidade encontra previsão no art. 6º, I, do PL 5.276/2016. Neste sentido, todo o anteprojeto deve ser interpretado à luz dessa principiologia, que não deixa de ser uma forma de controle assegurada ao titular. Destarte, por exemplo, o inciso III, do art. 16, que autoriza a transferência de dados a terceiro deve ser lido em consonância com o citado princípio, na medida em que é direito do titular o acesso à informação, ganhando relevo no caso a finalidade específica do tratamento, os sujeitos receptores dos dados e o âmbito de difusão, nos termos do art. 8º, incisos I e V, do projeto. Além da finalidade informada, o compartilhamento e, por conseguinte, o tratamento não poderão se dar.

O regulamento jurídico da matéria no PL 4.060/2012, por seu turno, autoriza o compartilhamento de dados, inclusive para fins comerciais, com empresas integrantes de um mesmo grupo econômico, parceiros comerciais ou terceiros que direta ou indiretamente contribua para o tratamento de dados pessoais, conforme o art. 14. Igualmente, no seu art. 16, também existe o permissivo legal para o compartilhamento, mas restrito a finalidades históricas, estatísticas ou de pesquisa científica.

Emerge como distinção nos dois regimes a densidade de direitos, mecanismos e garantias assegurados ao titular dos dados no PL 5.276/2016, sobretudo pela expressa menção e vinculação ao princípio da finalidade e o próprio parâmetro da transparência, ao passo que o PL 4.060/2012, com o rol de direitos do titular limitado, sequer prevê os princípios próprios para a tutela dos dados, a despeito dos dois anteprojetos autorizarem o compartilhamento.

5.7 Mecanismos de controle

A tutela dos dados pessoais, na esteira da sua quarta geração de leis, não prescinde de mecanismos de controle em níveis coletivo e individual, valendo-se da premissa elencada por Rodotá como necessária à adequada proteção das informações. Trata-se, em realidade, do controle do corpo eletrônico da pessoa, em vista da sua autodeterminação.[15]

Na perspectiva do titular dos dados, impende ressaltar o Capítulo III do PL 5.276/2016, sobretudo o seu art. 18, associado aos direitos titularizados pelo particular, no

[15] A perspectiva do controle deve ser analisada pela tríade de ferramentas protetivas da privacidade destacada por Daniel Buscar, em que se identificam os controles espacial, contextual e temporal. Pelo controle espacial, na esteira da autodeterminação informativa, é possibilitado ao indivíduo ter exata e prévia ciência do espaço informacional sobre o qual desenvolverá sua personalidade. Pelo controle contextual assegura-se a ciência quanto à exatidão da informação, a qual, quando divulgada, deverá assegurar o correto contexto em que foi recebida. O controle temporal, por sua vez, demanda a proteção das escolhas pessoais após certo período de tempo, fortemente associado ao direito ao esquecimento. (BUSCAR, Daniel. Controle temporal de dados: o direito ao esquecimento. *Civilistica.com*. Rio de Janeiro, a. 2., n. 3., jul.-set./2013. Disponível em: http://civilistica.com/controle-temporal-de-dados-o-direito-ao-esquecimento/. Acesso em: 15 ago. 2017, p. 7-10).

qual se observa, como dito, uma concretização do regime principiológico da proteção de dados, marcadamente do princípio do livre acesso. Registre-se também a previsão de mecanismos de controle dispersos pelo anteprojeto, a exemplo do parágrafo 2º, do art. 10.

Deveras, o art. 20 do citado projeto assegura ao titular o direito de solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive nas que dizerem respeito à definição de perfil ou à avaliação de aspectos da personalidade, porquanto verificada a necessidade de um meio de controle específico quando o tratamento de dados associar-se a formas de estigmatização social e, por consequência, significar um vetor de mitigação do livre desenvolvimento da pessoa.

Ratifica-se, igualmente, a impossibilidade dos dados pessoais referentes ao exercício regular de direitos do titular serem utilizados em seu desfavor no art. 21, bem como no art. 22 é reiterada a possibilidade de recurso à autoridade judiciária, individual ou coletivamente, valendo-se da disciplina já existente como o *habeas data* (Lei n. 9.507 de 1997), o Código de Defesa do Consumidor (Lei n. 8.078 de 1990), especialmente de seus artigos 81 e 82 que tratam dos direitos metaindividuais ou coletivos *lato sensu*, e a Ação Civil Pública (Lei n. 7.347 de 1985), como instrumento basilar do microssistema processual coletivo brasileiro.

No que tange ao PL 4.060/2012, verificou-se em seu art. 5º a menção à possibilidade de defesa do direito à proteção de dados também a título coletivo ou individual, oportunidade em realizou-se remissão de forma não exauriente ao Código de Defesa do Consumidor e à Lei da Ação Civil Pública.

Com relação aos direitos do titular, o regime jurídico do PL 4.060/2012 é demasiadamente inferior ao outro projeto analisado e dissonante dos *Fair Information Principles*, notadamente porque basicamente cingem-se à possibilidade de bloqueio do tratamento dos dados pessoais, salvo se tal for realizado com o escopo de assegurar a execução de obrigações legais ou contratuais, bem como garante o acesso dos particulares à política de privacidade do responsável pelo tratamento dos dados, conforme os artigos 19 e 20, inexistindo qualquer referência à concretização do princípio do livre acesso. Não obstante, o direito à autodeterminação informativa é previsto genericamente no art. 13, sem a previsão de instrumentos concretos com aptidão para tanto.

Noutro quadrante, como elencado por Rodotá (2008, p. 60), o controle na esfera coletiva não prescinde de uma autoridade administrativa independente para assegurar o cumprimento da lei, o que acaba por ser consentâneo com o conceito de *enforcement*, eventualmente dotada de poderes para adaptar a situações particulares os princípios previstos nas cláusulas gerais. De fato, a proteção deve usurpar da atribuição de poderes unicamente

aos interessados diretos, abarcando também a concessão de um poder geral de vigilância a órgãos criados especificamente para a proteção de dados.

Neste ponto, a diferença entre os Projetos de Lei n. 4.060/2012 e o 5.276/2016 é profunda, posto que no primeiro não há qualquer menção a um órgão específico para tal fim nos termos indicados por Rodotá, ao passo que no segundo, no Capítulo VIII que versa sobre a fiscalização, identifica-se a Seção II que faz expressa previsão de um órgão com essa finalidade, identificando suas atribuições no art. 53, com competência normativa autônoma, bem como de um Conselho Nacional de Proteção de Dados e Privacidade, disciplinado nos artigos 54 e 55. Anote-se que inclusive as operações de tratamento realizadas pelo Poder Público estariam sujeitas a tal controle, nos moldes do art. 29, do projeto, bem como a medidas específicas de responsabilização, como regulamentado na Seção II, do Capítulo IV.[16]

Deve-se dispensar atenção, todavia, à forma de constituição do Conselho Nacional de Proteção de Dados e Privacidade prevista no art. 54, do PL 5.276/2016, que com uma composição de quinze titulares, acrescidos dos respectivos suplentes, deve ser, nos termos da lei, integrado por sete representantes titulares do Poder Executivo federal, como dispõe o inciso I.

Ao tecer considerações sobre o modelo da autoridade administrativa, Rodotá (2008, p. 86) adverte que deve ser garantida sua independência em relação ao Poder Executivo, uma vez que entre as funções mais delicadas dos organismos de controle se encontra a de intervir nos bancos de dados diretamente associados à ação do governo. Minimamente, a composição do órgão não deveria se dar de forma que fosse garantido um papel determinante às pessoas nomeadas pelo Executivo, sob pena de comprometer a credibilidade da ação de vigilância.

Ademais, sustenta o autor que o vínculo institucional de tais órgãos deveria ser constituído pelas assembleias parlamentares, de modo a garantir a publicidade e a efetiva discussão acerca das posições assumidas. Pelo que se depreende do inciso II, do art. 54, do referido projeto, o Conselho seria composto de apenas um representante do Congresso Nacional, o que além de desproporcional com o número de representantes do Poder Executivo, é significativo da prioridade de poder que se busca conceder com tal previsão.

Aduz Rodotá que necessário se faz que o órgão de controle se situe fora das estruturas administrativas e burocráticas tradicionais, posto que são justamente as que

[16] Determina o art. 29 que "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". (BRASIL. Projeto de Lei n. 5.276, de 13 de maio de 2016 da Câmara dos Deputados, cit., p. 12).

promovem largamente a coleta de dados, na medida em que a função de vigilância deve ser estruturada de forma a obedecer a uma lógica distinta daquela dos sujeitos a serem controlados.

No que concerne às atribuições desses órgãos de vigilância, depreendidas de experiências conhecidas, como aponta Rodotá (2008, p. 87), podem ser citadas as funções de "cães de guarda" da legalidade da ação de quem coleta, trata e circula informações, seja munido de um poder de autorização geral ou especial ou através de uma ação de vigilância nesta área; organismos consultivos do setor público ou privado, também com o escopo de facilitar práticas consensuais para a fixação de regras para a circulação das informações; instituições de resolução e/ou de atenuação de conflitos e organismos dotados de poder normativo autônomo ou regulamentar de adaptação dos princípios previstos legalmente.

Depreende-se do rol do art. 54, do PL 5.276/2016, que não é exaustivo, consoante o inciso XIII, que tais funções são contempladas, no entanto, não existe menção expressa à competência de resolução ou atenuação de conflitos o que, contudo, não pode ser afastado em termos de uma interpretação ampla do dispositivo.

O PL 4.060/2012, por sua vez, apenas faz previsão da possibilidade de instituição de Conselhos de Autorregulamentação pelas entidades representativas de responsáveis pelo tratamento, para formular códigos que definirão parâmetros éticos para tratamento de dados, comunicação comercial e condições para sua organização, funcionamento, controle e sanções. Na justificativa do anteprojeto, foi asseverado que o Estado deve cuidar de questões gerais, mas que "a sociedade é refratária ao excesso de tutela por parte do Estado e que deseja exercer na plenitude seus direitos constitucionais" (BRASIL, 2012, p. 8).

Cediço é que uma tutela efetiva da proteção de dados não dispensa mecanismos efetivos de controle, entretanto, o mencionado projeto, além de relegar tal incumbência aos responsáveis pelas operações que são sujeitos parciais, não desvinculou as figuras de controlador e controlado. Não bastasse, situou tal instituto na esfera da faculdade, o que é incompatível com um ambiente jurídico adequado à tutela das informações, mormente em se tratando do direito fundamental à proteção de dados, visto que não se desconsidera a assimetria do poder e de que muito pode ser falacioso um discurso de liberdade nestes termos.

Ante essas considerações, infere-se que o PL 4.060/2012 apresenta significativas deficiências na esfera do controle, seja de forma difusa, pela atribuição de mecanismos aptos aos titulares, cidadãos e grupos, seja pela perspectiva concentrada, notadamente verificada a ausência de previsão de uma autoridade administrativa efetiva em vista da noção de *enforcement*.

Registre-se que a formulação de regras de boas práticas pelos responsáveis pelo tratamento de dados pessoais, individualmente ou por meio de associações, com finalidades similares aos Conselhos de Autorregulamentação previstos no PL 4.060/2012, também encontra prescrição no art. 50, do PL 5.276/2016, a indicar um regime jurídico de controle mais desenvolvido.

CONCLUSÃO

A concretização do princípio da dignidade humana, na conjuntura das sociedades de informação e dos avanços tecnológicos, demanda o estabelecimento de um regime jurídico adequado à circulação das informações, especialmente no que tange aos dados pessoais, uma vez considerada a compreensão do corpo da pessoa em uma perspectiva física e outra eletrônica, ambos carecedoras de tutela.

O alicerce desta compreensão se situa na alteração qualitativa do conceito de privacidade, eminentemente complexo, que excedeu a acepção clássica do direito de ser deixado só, para integrar a noção de autodeterminação informativa, de modo a assegurar à pessoa a livre construção da própria esfera privada, fora de uma lógica cristalizada e de estigmatizações, sobretudo no âmbito dos dados sensíveis. Destarte, desenvolveu-se para além da privacidade o direito fundamental à proteção de dados, que demandando uma proteção dinâmica, não prescinde de um regime jurídico próprio.

A despeito da tutela dos dados pessoais se dar de forma pontual no ordenamento jurídico brasileiro, não está em vigor no Brasil uma legislação geral para a proteção de dados, ensejo que fundamenta variadas iniciativas parlamentares, dentre as quais se destacaram os Projetos de Lei n. 4.060 de 2012 e 5.276 de 2016, com trâmite conjunto na Câmara dos Deputados.

Com o escopo de analisar institutos versados nos anteprojetos e a consonância com um ambiente jurídico adequado à tutela das informações, máxime dos dados pessoais sensíveis, o estudo desenvolvido objetivou destacar os pontos de maior relevo nas construções legislativas, com caráter marcadamente exploratório da construção do regime jurídico do direito fundamental à proteção de dados, porquanto a matéria demanda continuados avanços de pesquisa.

Em relação aos Projetos de Lei n. 4.060 de 2012 e 5.276 de 2016 examinados, é possível asseverar que ambos estabelecem uma disciplina específica para a tutela dos dados sensíveis, sem embargo, o segundo possui uma moldura jurídica mais densificada e protetiva

que o outro, bem como uma maior consonância com um ambiente normativo adequado à tutela dos dados pessoais, em que pese a necessidade de se repensar alguns de seus institutos e interpretá-los pelo filtro da dignidade da pessoa humana.

De plano, verificou-se que as duas construções legislativas apresentaram um conceito limitado de dados sensíveis, uma vez que na medida em que a natureza sensível de um dado advém de sua aptidão para gerar situações de discriminação e desigualdade, a tutela da pessoa deve se concretizar mediante uma cláusula geral para assegurar a sua dignidade, como corolário do art. 1º, III, da Constituição da República Federativa do Brasil de 1988, principalmente em seu componente da liberdade substancial.

Adotando um regime principiológico próprio da proteção de dados, o Projeto de Lei n. 5.276/2016 disciplinou um rol específico de direitos assegurados ao respectivo titular, realizou atribuições a uma autoridade administrativa independente, bem como a um Conselho Nacional de Proteção de Dados e Privacidade, como mecanismos de controle concentrado, não se olvidando do controle difuso de competência dos particulares. No tangente ao citado Conselho, ressalvou-se, entretanto, a constituição majoritária de membros do Poder Executivo federal, o que se revelou inadequado pela possível confusão entre as figuras de controlador e controlado, notadamente em vista da frequente coleta de dados por parte do Estado.

Outrossim, o Projeto de Lei n. 5.276/2016 realizou atribuições a legislação específica, como no caso de segurança pública, bem como prescreveu recurso à autoridade judiciária para assegurar a tutela dos dados pessoais.

Por seu turno, o Projeto de Lei n. 4.060/ 2012 não dispôs sobre um regime de princípios próprios da proteção de dados, apresentou exíguo rol de direitos e mecanismos facultados ao particular e, com relação à perspectiva de controle, padeceu de uma regulamentação efetiva no que concerne aos instrumentos concedidos ao titular, tendo relegado o controle no âmbito coletivo à mera faculdade dos responsáveis pelo tratamento de dados, em uma vertente evidentemente parcial e, portanto, inapta a exercer um poder de vigilância.

Noutro giro, o Projeto de Lei n. 5.276/2016 vedou o tratamento dos dados sensíveis, no entanto, excetuou a regra e estabeleceu condições específicas para o consentimento neste mister, bem como nas demais hipóteses de dispensa de consentimento, devendo prevalecer, em qualquer caso, a impossibilidade de tratamento de dados em desfavor do titular, ressalvada a previsão de legislação especial a ser interpretada restritivamente. Com referência ao Projeto de Lei n. 4.060/2012, o tratamento de dados sensíveis ficou condicionado à autorização do

particular, sem requisitos específicos para a sua legitimação, ou à imposição legal, de forma genérica, o que é perigoso, uma vez considerada a assimetria de poder entre os envolvidos.

Os enfoques a serem considerados nos anteprojetos analisados são diversos, tendo o presente estudo se voltado para a investigação dos dados sensíveis e dos institutos que neles repercutem de forma incisiva. Em realidade, o tema merece, como ressaltado, aprofundadas pesquisas e debates, inclusive em outras áreas do conhecimento, mormente em se considerando a necessária previsão de instrumentos prospectivos aptos a garantir o pleno exercício da dignidade da pessoa humana na conjuntura do tecido social cada vez mais tecnológico.

A construção de um ambiente jurídico apto a concretizar a constitucionalização da pessoa apenas pode ser verificada na medida em que a valorização das situações existenciais encontra campo propício ao pleno e livre desenvolvimento da personalidade, ao que deve se submeter um regime geral do direito fundamental à proteção de dados, sobretudo dos dados sensíveis, sob o primado da Constituição da República e, destarte, do fundamento da dignidade da pessoa humana.

REFERÊNCIAS

BAIÃO, Kelly Sampaio; GONÇALVES, Kalline Carvalho. *A garantia da privacidade na sociedade tecnológica*: um imperativo à concretização do princípio da dignidade da pessoa humana. Civilistica.com. Rio de Janeiro, a. 3, n. 2, jul.-dez./2014. Disponível em: <http://civilistica.com/a-garantia-da-privacidade-na-sociedade-tecnologica-um-imperativo-a-concretizacao-do-principio-da-dignidade-da-pessoa-humana/>. Acesso em: 15 ago. 2017.

BARROSO, Luís Roberto. *A dignidade da pessoa humana no direito constitucional contemporâneo:* natureza jurídica, conteúdos mínimos e critérios de aplicação. Versão provisória para debate público. Mimeo., dezembro de 2010, p. 1-39. Disponível em: <http://www.luisrobertobarroso.com.br/wp-content/uploads/2010/12/ Dignida-de_texto-base_11dez2010.pdf.> Acesso em: 10 set. de 2017.

BELLUCK, Pam. To Try to Net Killer, Police Ask a Small Town's Men for DNA. *New York Times*. Boston. 10 jan. 2005. Disponível em: <http://www.nytimes.com/2005/01/10/us/to-try-to-net-killer-police-ask-a-small-towns-men-for-dna.html>. Acesso em: 09 set. 2017.

BRANDEIS, Louis; WARREN, Samuel. *The right do privacy*. Harvard Law Review, vol. 4, 1890.

BRASIL. Constituição da República Federativa do Brasil de 05 de outubro de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 25/09/2017.

_____. Lei n. 12527, de 18 de novembro de 2011. *Lei de Acesso à Informação*. Brasília, Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 10 set. 2017.

_____. Lei n. 12965, de 23 de abril de 2014. *Marco Civil da Internet*. Brasília, Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 10 set. 2017.

_____. Lei nº 7347, de 12 de novembro de 1997. *Lei da Ação Civil Pública*. Brasília, Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L7347orig.htm>. Acesso em: 10 set. 2017.

_____. Lei n. 8078, de 11 de setembro de 1990. *Código de Defesa do Consumidor*. Brasília, Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8078.htm>. Acesso em: 10 set. 2017.

_____. Lei n. 9507, de 12 de novembro de 1997. *Lei do Habeas Data*. Brasília, Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9507.htm>. Acesso em: 10 set. 2017.

_____. Projeto de Lei n. 4.060, de 13 de junho de 2012 (da Câmara dos Deputados). Brasília, Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=4B1D896E8D2C95FCDB947867FC29F87D.proposicoesWebExterno1?codteor=1001750&filename=PL+4060/2012>. Acesso em: 10 set. 2017.

_____. Projeto de Lei n. 5.276, de 13 de maio de 2016 (da Câmara dos Deputados). Brasília, Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1457459&filename=PL+5276/2016>. Acesso em: 10 set. 2017.

BUSCAR, Daniel. Controle temporal de dados: o direito ao esquecimento. *Civilistica.com*. Rio de Janeiro, a. 2., n. 3., jul.-set./2013. Disponível em: http://civilistica.com/controle-temporal-de-dados-o-direito-ao-esquecimento/. Acesso em: 15 ago. 2017.

CONSELHO DA EUROPA. *Convenção Para A Protecção das Pessoas Relativamente Ao Tratamento Automatizado de Dados de Carácter Pessoal*. Disponível em: <https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm>. Acesso em: 10 set. 2017.

DONEDA, *Danilo. Avanço tecnológico muda o conceito de dados anônimos ou sensíveis.* S. I.: Cdtv Convergência Digital, 2016. (18 min.), son., color. Disponível em: <https://www.youtube.com/watch?v=dLCc8SEAa7w>. Acesso em: 13 set. 2017.

_____. *A proteção dos dados pessoais como um direito fundamental.* Espaço Jurídico, Joaçaba, v. 12, n. 2, p. 91-108, jul/dez 2011. Disponível em: <http://editora.unoesc.edu.br/index.php/espacojuridico/article/download/1315/658>. Acesso em: 01 set. 2017.

G1. Entenda o caso de Edward Snowden, que revelou espionagem dos EUA. *G1*. São Paulo. 02 jul. 2013. Disponível em: <http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>. Acesso em: 15 set. 2017.

KONDER, Carlos Nelson. Vulnerabilidade patrimonial e vulnerabilidade existencial: por um sistema diferenciador. *Revista de Direito do Consumidor*, v. 99, p. 107, 2015.

MORAES, Maria Celina Bodin de. Ampliando os direitos da personalidade. In: *Na medida da pessoa humana*: estudos de direito civil-constitucional. Rio de Janeiro: Renovar, 2010.

_____. *Danos à pessoa humana, uma leitura civil-constitucional dos danos morais*, Rio de Janeiro: Renovar, 2003.

_____. O princípio da dignidade da pessoa humana. In: *Na medida da pessoa humana:* estudos de direito civil-constitucional. Riode Janeiro: Renovar, 2010, pp. 71-120.

RODOTÀ, Stefano. *A vida na sociedade da vigilância.* A privacidade hoje. Rio de Janeiro: Renovar, 2008.

_____. *Por que é necessária uma Carta de Direitos da Internet?*. Trad. Bernardo Diniz Accioli de Vasconcellos e Chiara Spadaccini de Teffé. Civilistica.com. Rio de Janeiro, a. 4, n. 2, jul.-dez./2015. Disponível em: <http://civilistica.com/wp-content/uploads/2015/12/Rodota%CC%80-trad.-de-Teffe%CC%81-e-Vasconcellos-civilistica.com-a.4.n.2.20152.pdf>. Acesso em: 01 set. 2017.

_____. Transformações do corpo. *Revista Trimestral de Direito Civil*, v. 19, p. 91-107.

SCHULMAN, Gabriel. www.privacidade-em-tempos-de-internet.com: o espaço virtual e os impactos reais à privacidade das pessoas. In TEPEDINO, Gustavo; TEIXEIRA, Ana Carolina

Brochado; ALMEIDA, Vitor (coords.). *O direito civil entre o sujeito e a pessoa:* estudos em homenagem ao professor Stefano Rodotá. Belo Horizonte: Fórum, 2016, pp. 330-360.

TEPEDINO, Gustavo. Normas constitucionais e direito civil na construção unitária do ordenamento. In: *Temas de Direito Civil*, t. III, Rio de Janeiro: Renovar, 2009.

TEPEDINO, Gustavo. O papel atual da doutrina do direito civil entre o sujeito e a pessoa. In: TEPEDINO, Gustavo; TEIXEIRA, Ana Carolina Brochado; ALMEIDA, Vitor (coords.). *O direito civil entre o sujeito e a pessoa:* estudos em homenagem ao professor Stefano Rodotá. Belo Horizonte: Fórum, 2016, pp. 17-35.

VIOLA, Mario; DONEDA. Danilo; CÓRDOVA, Yasodara; ITAGIBA, Gabriel. Entre a privacidade e a liberdade de informação e expressão: existe um direito ao esquecimento no Brasil? In TEPEDINO, Gustavo; TEIXEIRA, Ana Carolina Brochado; ALMEIDA, Vitor (coords.). *O direito civil entre o sujeito e a pessoa:* estudos em homenagem ao professor Stefano Rodotá. Belo Horizonte: Fórum, 2016, pp. 361-380.

ANEXOS

ANEXO A – Projeto de Lei n. 4.060 de 2012 da Câmara dos Deputados

PROJETO DE LEI Nº. , de 2012

(Do Sr. Deputado MILTON MONTI)

Dispõe sobre o tratamento de dados pessoais, e dá outras providências.

O Congresso Nacional decreta:

TÍTULO I

Da Tutela dos Dados Pessoais

CAPÍTULO I

Disposições Gerais

Art. 1º. Esta lei tem por objetivo garantir e proteger, no âmbito do tratamento de dados pessoais, a dignidade e os direitos fundamentais da pessoa natural, particularmente em relação a sua liberdade, privacidade, intimidade, honra e imagem.

Art. 2º. Toda pessoa tem direito a proteção de seus dados pessoais.

Art. 3º. A proteção aos direitos e garantias mencionados no artigo primeiro desta lei deverá ser promovida com observância dos princípios constitucionais da Defesa do Consumidor, Livre iniciativa, Liberdade de Comunicação e Ordem Econômica, nos termos dos artigos 1º, IV, 5º, inc. IX, XXXII, 170 e 220 da Constituição Federal.

Art. 4º. A presente lei aplica-se aos tratamentos de dados pessoais realizados em território nacional, por pessoa física ou jurídica, de direito público ou privado, ainda que o correspondente banco de dados, representado por arquivos, registros ou quaisquer outras bases de processamento, esteja, permanente ou provisoriamente, armazenado em território estrangeiro.

Art. 5º. A defesa dos interesses e direitos dos titulares de dados poderá ser exercida em juízo individualmente ou a título coletivo, na forma do disposto no artigo 81 e 82 da Lei 8.078, de 11 de setembro de 1990, da Lei 7.347 de 24 de julho de 1985 e nos demais instrumentos legais.

Art. 6º. Esta lei não se aplica:

I – aos bancos de dados utilizados para o exercício regular da atividade jornalística;

II – aos dados relativos a pessoas físicas, quando se referirem, exclusivamente, a informações relativas às suas atividades profissionais e/ou comerciais;

III - aos bancos de dados utilizados para a pesquisa histórica, científica ou estatística, de administração pública, investigação criminal ou inteligência;

IV – ao tratamento de dados pessoais de informações de domínio público.

Art. 7º. Para os fins da presente lei, entende-se como:

I – dado pessoal: qualquer informação que permita a identificação exata e precisa de uma pessoa determinada;

II – tratamento de dados: toda operação ou conjunto de operações, realizadas com ou sem o auxílio de meios automatizados, que permita o

armazenamento, ordenamento, conservação, atualização, comparação, avaliação, organização, seleção, extração de dados pessoais;

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

IV - dados sensíveis: informações relativas à origem social e étnica, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas do titular;

V - responsável: a pessoa natural ou jurídica, de direito público ou privado, a quem compita, na qualidade de possuidora de arquivo, registro, base ou banco de dados, a tomada de decisões referentes à realização de tratamento de dados pessoais;

VI – interconexão: transferência de dados pessoais de um banco de dados a outro;

VII – bloqueio: suspensão temporária ou permanente de qualquer operação de tratamento realizada sobre dados pessoais específicos ou sobre a integralidade de um ou mais bancos de dados.

Art. 8º. A veracidade e regularidade dos dados pessoais fornecidos para tratamento é de responsabilidade do titular dos dados, presumindo-se a sua acuidade, correção e veracidade. A realização de operações de tratamento de dados pessoais não implica responsabilidade pela verificação da veracidade, exatidão ou correção dos dados.

CAPÍTULO II

Dos Requisitos para Tratamento de Dados Pessoais

Art. 9º . Os dados pessoais serão tratados com lealdade e boa fé, de modo a atender aos legítimos interesses dos seus titulares.

Art. 10. A disciplina jurídica do tratamento de dados pessoais tem como objetivos fundamentais a proteção dos direitos básicos do consumidor, a garantia da ordem econômica e

a manutenção da livre iniciativa e da liberdade de comunicação, de modo que em seu âmbito deverão ser observados os princípios estabelecidos nesta lei.

Art. 11. O responsável pelo tratamento de dados, bem como eventuais subcontratados, deverão adotar medidas tecnológicas aptas a reduzir ao máximo o risco da destruição, perda, acesso não autorizado ou de tratamento não permitido pelo titular.

Parágrafo Único. As medidas a serem adotadas devem ser proporcionais ao atual estado da tecnologia, à natureza dos dados e às características específicas do tratamento, em particular no caso do tratamento de dados sensíveis.

Art. 12. O início do tratamento de dados pessoais sensíveis, quando não solicitado pelo titular, somente ocorrerá mediante autorização deste, por qualquer meio que permita a manifestação de sua vontade, ou na hipótese de imposição legal.

Art. 13. O tratamento de dados pessoais ou a sua interconexão respeitará a lealdade e boa fé, de modo a atender aos legítimos interesses dos seus titulares, lhes devendo ser garantido sempre o direito ao bloqueio do registro, salvo se necessário para cumprimento de obrigação legal ou contratual.

Art. 14. Respeitado o disposto no artigo anterior, os responsáveis pelo tratamento de dados poderão compartilhá-los, inclusive para fins de comunicação comercial, com empresas integrantes de um mesmo grupo econômico, parceiros comerciais ou terceiros que direta ou indiretamente contribuam para a realização do tratamento de dados pessoais.

Art. 15. O Titular tem direito a autodeterminação das informações e dados pessoais prestados ou coletados, por qualquer meio.

Parágrafo Único. O tratamento de dados e o envio de comunicações comerciais ou sociais é permitido, salvo se o titular solicitar o bloqueio do tratamento dos seus dados ou tiver manifestado diretamente ao responsável pelo envio a opção de não recebê-la.

Art. 16. Quando do término ou bloqueio do tratamento dos dados pessoais, o responsável poderá conservá-los ou compartilhá-los com terceiros, somente quando tais práticas sejam adotadas para finalidades históricas, estatísticas ou de pesquisa científica.

Art. 17. O tratamento de dados pessoais de crianças somente será possível mediante o consentimento dos seus pais, responsáveis legais ou por imposição legal.

Art. 18. É vedada a captura, o tratamento ou a manutenção de dados pessoais obtidos por meio de dolo ou coação.

CAPÍTULO III

Dos Direitos do Titular

Art. 19. O titular poderá, a qualquer momento, requerer o bloqueio do tratamento de seus dados pessoais, salvo se a manutenção do tratamento for necessária à execução de obrigações legais ou contratuais.

Art. 20. Os responsáveis pelo tratamento de dados deverão assegurar, aos titulares dos dados pessoais, amplo acesso à sua política de privacidade, que deverá apresentar informações acerca da utilização dos dados coletados.

TÍTULO II

Da Tutela Fiscalizatória e Sancionatória

Art. 21. Os responsáveis pelo tratamento de dados pessoais que incorrerem em infração às normas estabelecidas pela presente lei, ficam sujeitos à aplicação das sanções previstas no Código de Defesa do Consumidor, sem prejuízo das demais sanções de natureza civil e penal cabíveis.

Art. 22. Sem prejuízo das sanções cabíveis, os órgãos e entidades previstos no artigo 82 da Lei 8.078/90, além das associações legalmente constituídas há pelo menos 1 (um) ano, poderão promover a celebração de Compromissos de Ajustamento de Conduta (CAC) com responsáveis que incorram em infração às normas desta lei, visando a adoção de medidas corretivas que considerem necessárias para reverter os efeitos danosos que a conduta infratora tenha causado e para evitar que esta se produza novamente no futuro.

Art. 23. As entidades representativas de responsáveis pelo tratamento de dados pessoais poderão instituir Conselhos de Autorregulamentação, que formularão códigos que definirão parâmetros éticos para tratamento de dados, comunicação comercial, bem como condições para sua organização, funcionamento, controle e sanções.

TÍTULO III

Das Disposições Finais e Transitórias

Art. 24. Os direitos e obrigações previstos nesta lei não excluem outros, decorrentes de tratados ou convenções internacionais de que o Brasil seja ou venha a ser signatário, da legislação interna ordinária, bem como de regulamentos expedidos pelas autoridades administrativas competentes.

Art. 25. Esta lei entra em vigor noventa dias após sua publicação.

JUSTIFICATIVA

O presente Projeto de lei tem por objetivo dar ordenamento jurídico e institucional ao tratamento de dados pessoais, bem como a proteção dos direitos individuais das pessoas, de acordo com a Constituição da República Federativa do Brasil.

O tratamento de dados é hoje uma realidade cada vez mais presente em nosso cotidiano, especialmente quando experimentamos o avanço da tecnologia da informação, em especial a internet e suas aplicações nas mais diversas áreas de nossa vida em sociedade. Até pouco tempo era inimaginável pensar nas aplicações e a interação que a internet teria em nosso dia-a-dia, ao mesmo tempo em que podemos imaginar que isso continuará em ritmo acelerado e de incremento, tendo em vista a velocidade em que novas tecnologias são desenvolvidas para a comunicação com as pessoas.

Dentro dessa realidade se faz necessário estabelecer normas legais para disciplinar tais relações, especialmente para dar proteção à individualidade e a privacidade das pessoas, sem impedir a livre iniciativa comercial e de comunicação.

Por esses motivos e sensibilizado pela realização do V Congresso Brasileiro da Indústria da Comunicação, evento promovido pela ABAP – Associação Brasileira das Agências de Publicidade e pelo FORCOM – Fórum Permanente de Comunicação, no qual tive a honra e a oportunidade de participar, e de forma especial como Presidente da Comissão 5 que tratou do tema da comunicação “one-to-one” Personalização X Privacidade, e que decidi apresentar o presente Projeto de Lei.

Debatemos com muitos especialistas dessa área, destacando aqui a participação do blogueiro Marcelo Tás, do ator Odilon Wagner, do Presidente da ABEMD Efraim Kapulski, do Advogado Vitor Morais de Andrade, do Diretor da Editora Abril Fernando Costa, além de mais de uma centena de participantes, sendo elaborado ao final e aprovado um relatório pelos participantes de Comissão, bem como a aprovação por todas as 38 entidades que compuseram o V Congresso em uma votação plenária, destacando ainda que o texto final foi aprovado por unanimidade.

Procurei no presente Projeto de Lei expressar o resultado de todos os debates e observações vindas das acaloradas reflexões daquele encontro. Podemos destacar as linhas mestras das conclusões dos debates que indicaram a necessidade de um marco regulatório para disciplinar essa atividade e que o mesmo deveria ser, geral e abrangente, face às mutações permanentes em uma área de evolução tecnológica tão rápida, bem como que as questões específicas deveriam ficar a cargo de um conselho de autorregulamentação, aos moldes do CONAR que é destaque em eficiência aqui em nosso país como também em outros países do mundo.

Não há dúvida nenhuma que o Estado deve cuidar das questões gerais, mas é também evidente que a sociedade é refrataria ao excesso de tutela por parte do Estado e que deseja exercer na plenitude seus direitos constitucionais inclusive o de receber se quiser comunicações pelos meios disponíveis no momento.

Desta forma gostaria de pedir aos meus pares que possam aprovar a presente propositura.

Sala das sessões em, de 2012

Deputado MILTON MONTI

ANEXO B – Projeto de Lei n. 5.276 de 2016 da Câmara dos Deputados

PROJETO DE LEI 5276/2016

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

A PRESIDENTA DA REPÚBLICA faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

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.

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 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.

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;

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.

CAPÍTULO II

REQUISITOS PARA O TRATAMENTO DE DADOS PESSOAIS

Seção I

Requisitos para o tratamento

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

I - mediante o fornecimento 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.

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.

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.

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.

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, dados utilizados para a formação do perfil comportamental de uma determinada pessoa natural, ainda que não identificada.

§ 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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

CAPÍTULO VII

DA SEGURANÇA E DAS BOAS PRÁTICAS

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.

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.

CAPÍTULO VIII
DA FISCALIZAÇÃO

Seção I
Sanções administrativas

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.

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 transacional;

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.

Brasília,

EMI nº 00073/2016 MJ MP

Brasília, 29 de Abril de 2016

Excelentíssima Senhora Presidenta da República,

1. Submetemos à elevada consideração de Vossa Excelência a minuta de Projeto de Lei que dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural.

2. O Anteprojeto é resultado de um amplo debate público promovido pelo Ministério da Justiça, que teve duração de quase seis meses, recebendo mais de 50 mil visitas e obtendo mais de 1.100 contribuições. Esses subsídios foram analisados e consolidados no texto ora apresentado pelo Ministério da Justiça em parceria com o Centro de Estudos sobre Tecnologias Web (Ceweb), vinculado ao Núcleo de Informação e Coordenação do Ponto BR (Nic.br) e com o Instituto Nacional de Ciência e Tecnologia para a Web (InWeb), da Universidade Federal de Minas Gerais.

3. A proposta visa assegurar ao cidadão o controle e a titularidade sobre suas informações pessoais, com fundamento na inviolabilidade da intimidade e da vida privada, na liberdade de expressão, comunicação e opinião, na autodeterminação informativa, no desenvolvimento econômico e tecnológico, bem como na livre iniciativa, livre concorrência e defesa do consumidor. O avanço da tecnologia da informação amplia enormemente o potencial de coleta, processamento e utilização de dados pessoais, o que representa, por um lado, uma oportunidade de geração de novos conhecimentos e serviços mas, por outro, pode acarretar graves riscos aos direitos da personalidade do cidadão, ao acesso a serviços e bens, além de uma grande insegurança jurídica para o ambiente de negócios de tecnologia da informação existente no país, bem como para o comércio exterior, por conta da desconformidade da legislação brasileira atual aos padrões internacionais existentes neste tema.

4. É relevante apontar que o debate sobre privacidade e dados pessoais de que trata este Anteprojeto de Lei também foi fortemente influenciado pelo contexto internacional, consubstanciado, por exemplo, pela Resolução da ONU de 25 de novembro de 2013 sobre "Direito à Privacidade na Era Digital". Nessa manifestação, o governo brasileiro se empenhou para criar medidas que reiterassem também "online" os direitos que os cidadãos possuem "offline". Ocorre, no entanto, que apesar dos esforços diplomáticos realizados pelo país nesse sentido, o Brasil encontra-se defasado em relação ao resto do mundo no que toca à regulamentação do tema, na medida em que ainda não possui qualquer lei específica que diga respeito à proteção de dados pessoais, enquanto cerca de 109 países possuem normas nesse sentido e mais de 90 destes têm uma autoridade pública específica especializada no tema.

5. Não é apenas pela defasagem em comparação a outros países que urge a necessidade de promulgação desta norma legal. A utilização, cada vez mais intensa, de dados pessoais na sociedade da informação cria um desequilíbrio entre os poderes dos indivíduos, titulares de seus próprios dados pessoais, e os dos utilizadores de tais dados, justamente pela quantidade de informações pessoais que as novas tecnologias são capazes de agregar e utilizar. Para que esses dados possam ser utilizados com fins transparentes e legítimos, ao mesmo tempo em que sejam garantidos os direitos de seus titulares, são

necessárias normas e mecanismos institucionais que estabeleçam os parâmetros e limites deste tratamento, até mesmo no momento de término dessa relação. Além disso, tendo em vista o caráter transnacional do fluxo dessas informações, cumpre indicar que este Projeto abrange tanto as operações de tratamento de dados pessoais realizadas no Brasil, como aquelas realizadas no exterior, mas cuja coleta tenha ocorrido em território nacional.

6. A minuta proposta abarca o tratamento de informações pessoais processadas tanto pelo setor público como pelo setor privado. Estão excluídos do âmbito de proteção da norma, no entanto, aqueles tratamentos de dados pessoais realizados para fins exclusivamente pessoais, bem como aqueles que tem por objeto o exercício regular da atividade jornalística, artística, literária ou acadêmica. Quanto à regulação referente à segurança pública, esta deverá respeitar os princípios gerais estabelecidos no texto, porém contará com legislação específica posterior a esta proposta.

7. Os direitos do titular, por sua vez, são explicitados, em particular com relação ao acesso, correção, dissociação e oposição ao tratamento de seus dados. Ademais, o anteprojeto estabelece normas específicas para o tratamento de dados cujo tratamento possa ensejar discriminação ao titular (os chamados "dados sensíveis", por se referirem a orientação sexual, convicções religiosas, filosóficas ou morais, ou opiniões políticas, por exemplo), prevendo como regra geral que esses dados não devem ser tratados e que ninguém pode ser obrigado a fornecer informações de tal natureza a seu respeito, ressalvadas as hipóteses previstas em lei, assim como um regramento mais rígido quando o tratamento desses dados for permitido.

8. Diante do exposto, fica claro que os dados pessoais merecem uma tutela forte e específica do ordenamento jurídico. O processamento dessas informações influencia diretamente a vida das pessoas, afetando oportunidades, escolhas e interações sociais, elementos que compõem o livre desenvolvimento da sua própria personalidade. Tendo isso em vista, é imperativo que haja um conjunto de princípios que norteiem o tratamento desses dados por terceiros, entre os quais podem ser destacados sua utilização somente para finalidades específicas, adequadas e necessárias, além da regra de que o responsável pela coleta desses dados deva mantê-los em segurança, e que não os utilize para discriminação e permita o acesso facilitado ao titular.

9. Além disso, são elencados uma série de requisitos para o tratamento dos dados pessoais, sem os quais este não pode se reputar legítimo. Um destes requisitos é o do consentimento livre e inequívoco do titular. Para garantir os direitos do titular, a decisão sobre o consentimento deve ser sempre livre e incontroversa para cada pessoa, sempre com base na boa-fé, de modo a preservar a sua autodeterminação e proteger a sua personalidade. Há, ainda, outros casos específicos para a legitimação do tratamento, como nos casos em que há legítimo interesse do titular. Essa exceção, por outro lado, não deve ser compreendida como uma escusa genérica à demanda do consentimento, mas sim deve estar atrelada a uma tutela específica, que não pode jamais reduzir direitos fundamentais do titular.

10. O estabelecimento de regras sobre a proteção de dados pessoais possui, portanto, duas funções: proteger o titular dos dados e, ao mesmo tempo, favorecer a sua utilização dentro de um patamar de segurança, transparência e boa-fé. Dessa forma, a utilização lícita de dados será incentivada pela delimitação de um espaço de segurança jurídica, favorecendo o fluxo de dados por agentes responsáveis e o desenvolvimento de setores econômicos ligados, por exemplo, às tecnologias de informação. Nesse sentido, a proposta também trata da transferência internacional de dados e o condicionamento de sua ocorrência para determinadas circunstâncias, entre elas, para países que tenham nível de proteção equiparável ao brasileiro. Essa disposição implica que a partir da promulgação da lei brasileira de proteção de dados pessoais, o país estará apto a entrar no rol de Estados com os quais as empresas europeias podem realizar negócios que envolvam o tratamento de dados pessoais, sendo um importante avanço para o comércio exterior e, portanto, para o desenvolvimento econômico do Brasil.

11. Com esse mesmo objetivo de garantir segurança jurídica nas relações entre titulares e usuários

de dados, a proposta inclui sanções administrativas para coibir abusos neste tratamento, indicando quais condutas são vedadas aos atores envolvidos nessa relação.

12. Não escapa também ao escopo do Anteprojeto de Lei, a necessidade de regulamentação da forma como o poder público deve tratar os dados pessoais da população. Nesses casos, as diretrizes gerais devem decorrer sempre de competências legais, e a transparência ativa sobre como são usados os dados por meio de sites públicos deve ser a regra.

13. É relevante indicar que este anteprojeto se constituirá no marco geral para a regulação da proteção e uso dos dados pessoais no país e se harmoniza com os instrumentos legais que atualmente tratam do tema de forma setorial ou específica no ordenamento jurídico brasileiro.

14. A aplicação efetiva do direito individual fundamental à privacidade depende, em grande medida, das respostas coletivas que serão apresentadas para implementá-lo, motivo pelo qual é necessário empenhar-se na construção de uma democracia da informação que proteja tanto a autodeterminação e a liberdade de controle das informações pessoais pelo cidadão, como também a tutela contra a utilização discriminatória dos dados. Nesse contexto, a minuta ora apresentada visa possibilitar que a sociedade brasileira obtenha os benefícios econômicos e sociais potencializados pela tecnologia da informação, ao criar no país uma arquitetura regulatória capaz de fazer emergir o tema da proteção de dados pessoais como um verdadeiro vetor de políticas públicas, composto por instrumentos estatutários, sancionatórios, bem como por um órgão administrativo, responsável pela implementação e aplicação da legislação.

15. Ainda, o texto abre espaço para que categorias profissionais e segmentos empresariais estabeleçam regras comuns, a título de boas práticas, outorgando ao mercado um grau necessário de autorregulamentação, sem prejuízo da observância aos princípios gerais da lei.

16. Com o objetivo de dar efetividade à regulamentação sugerida, a proposta prevê um órgão competente para a proteção de dados pessoais no país. Será sua responsabilidade elaborar diretrizes de uma Política Nacional de Proteção de Dados Pessoais e Privacidade, promover entre a população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais, bem como das medidas de segurança, estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, entre outras medidas.

17. Como auxiliar deste órgão, propõe-se a criação de um Conselho Nacional de Proteção de Dados Pessoais e Privacidade, composto por representantes do poder público, setor privado, academia, comunidade técnica e organizações não-governamentais.

18. A consolidação de um regime integrado de proteção de dados no Brasil mostra-se, assim, fundamental no ordenamento jurídico pátrio, de modo a possibilitar uma regulação integral do tema e a coesão de diversas iniciativas na área. Somente uma regulação geral assegurará a instituição de princípios harmônicos sobre o tema, proporcionando o controle dos riscos envolvidos no processamento de dados e assegurando o controle do cidadão em relação às suas próprias informações pessoais e, assim, garantindo a necessária segurança jurídica para a atividade empresarial e para a administração pública no tratamento de dados pessoais.

19. Essas, Senhora Presidenta, são as razões que justificam a apresentação do Anteprojeto de Lei que ora submetemos à elevada apreciação de Vossa Excelência.

Respeitosamente,

Assinado eletronicamente por: Eugênio José Guilherme de Aragão, Francisco Gaetani