Ministério da Justiça

UnB

Centro de Apoio ao Desenvolvimento Tecnológico

latitude
Laboratório de tecnologias da tomada de decisão

Termo de Cooperação/Projeto:

Acordo de Cooperação Técnica FUB/CDT e MJ/SE Registro de Identidade Civil – Replanejamento e Novo Projeto Piloto

Documento:

RT Levantamento da Legislação Aplicada ao Acesso a Dados Pessoais

Data de Emissão:

29/10/2015

Elaborado por:

Universidade de Brasília – UnB
Centro de Apoio ao Desenvolvimento Tecnológico – CDT
Laboratório de Tecnologias da Tomada de Decisão – LATITUDE.UnB

MINISTÉRIO DA JUSTIÇA

José Eduardo Cardozo
Ministro

Marivaldo de Castro Pereira
Secretário Executivo

Hélvio Pereira Peixoto
Coordenador Suplente do Comitê Gestor do SINRIC

UNIVERSIDADE DE BRASÍLIA

Ivan Marques Toledo Camargo
Reitor

Paulo Anselmo Ziani Suarez
Diretor do Centro de Apoio ao Desenvolvimento Tecnológico – CDT

Rafael Timóteo de Sousa Júnior
Coordenador do Laboratório de Tecnologias da Tomada de Decisão – LATITUDE

EQUIPE TÉCNICA
Ana Maria da Consolação Gomes Lindgren
Andréa Benoliel de Lima
Celso Pereira Salgado
Delluiz Simões de Brito
Elaine Fabiano Tocantins
Fernando Saliba Oliveira
Fernando Teodoro Filho
Guilherme Braz Carneiro
Joaquim de Oliveira Machado
José Alberto Sousa Torres
Marcelo Martins Villar
Raphael Fernandes de Magalhães Pimenta
Rodrigo Borges Nogueira
Rodrigo Gurgel Fernandes Távora
Sara Lais Rahal Lenharo

EQUIPE TÉCNICA
Flávio Elias Gomes de Deus (Pesquisador Sênior)
William Ferreira Giozza (Pesquisador Sênior)
Ademir Agustinho de Rezende Lourenço
Adriana Nunes Pinheiro
Alysson Fernandes de Chantal
Andréia Campos Santana
Antônio Claudio Pimenta Ribeiro
Carolinne Januária de Souza Martins
Daniela Carina Pena Pascual
Danielle Ramos da Silva
Diogenes Ferreira Reis Fustinoni
Fábio Lúcio Lopes Mendonça
Fábio Mesquita Buiati
Glaidson Menegazzo Verzeletti
Heverson Soares de Brito
Johnatan Santos de Oliveira
Kelly Santos de Oliveira Bezerra
Luciano Pereira dos Anjos
Luciene Pereira de Cerqueira Kaipper
Luiz Antônio de Souto Evaristo
Luiz Claudio Ferreira
Marco Schaffer
Marcos Vinicius Vieira da Silva
Pedro Augusto Oliveira de Paula
Roberto Mariano de Oliveira Soares
Sergio Luiz Teixeira Camargo
Soleni Guimarães Alves
Suzane Lais De Freitas
Valério Aymoré Martins
Vera Lopes de Assis
Wladimir Rodrigues da Fonseca

HISTÓRICO DE REVISÕES

Data	Versão	Descrição
25/09/2014	0.1	Versão inicial.
03/10/2014	0.2	Revisão e implementação de texto e forma.
15/10/2014	0.3	Revisão e implementação de texto e forma.
22/10/2014	0.4	Inclusão item 2 – Revisão de Texto.
06/11/2014	0.5	Revisão e implementação de texto e forma.
13/11/2014	0.6	Revisão e implementação de texto e forma.
17/11/2014	0.7	Inclusão item 3.
24/11/2014	0.8	Inclusão item 4.
27/11/2014	0.9	Revisão e implementação de texto e forma.
01/12/2014	0.10	Revisão e implementação de texto e forma.
04/12/2014	0.11	Entrega relatório
13/08/2015	0.12	Revisão do relatório
01/09/2015	0.13	Revisão e implementação de texto e forma.
29/10/2015	0.14	Versão pós nota técnica.

latitude
Laboratório de tecnologias da tomada de decisão

Universidade de Brasília – UnB
Campus Universitário Darcy Ribeiro - FT – ENE – Latitude
CEP 70.910-900 – Brasília-DF
Tel.: +55 61 3107-5598 – Fax: +55 61 3107-5590

SUMÁRIO

1. INTRODUÇÃO

A Secretaria Executiva (SE/MJ), vinculada ao Ministério da Justiça (MJ), é responsável por viabilizar o desenvolvimento e a implantação do Registro de Identidade Civil, instituído pela Lei nº 9.454, de 7 de abril de 1997, regulamentado pelo Decreto nº 7.166, de 5 de maio de 2010.

Atualmente, a República Federativa do Brasil conta com sistema de identificação de seus cidadãos amparado pela Lei nº 7.116, de 29 de agosto de 1983. Essa lei assegura validade nacional às Carteiras de Identidade, ou Cédulas de Identidade; confere também autonomia gerencial às Unidades Federativas no que concerne à expedição e controle dos números de registros gerais emitidos para cada documento. Essa condição de autonomia, ao contrário do que pode parecer, fragiliza o sistema de identificação, já que dá condições ao cidadão de requerer legalmente até 27 (vinte e sete) cédulas de identidades diferentes. Com essa facilidade legal, inúmeras possibilidades fraudulentas se apresentam de maneira silenciosa, pois, na grande maioria dos casos, os Institutos de Identificação das Unidades Federativas não dispõem de protocolos e aparato tecnológico para identificar as duplicações de registro vindas de outros estados, ou até mesmo do seu próprio arquivo datiloscópico. Consoante aos fatos, os Institutos de Identificação não trabalham interativamente para que haja trocas de informações de dados e geração de conhecimento para manuseio inteligente e seguro para individualização do cidadão em prol da sociedade.

Com foco na busca de soluções para tais problemas, o Programa RIC prevê a administração central dos dados biográficos e biométricos dos cidadãos no Cadastro Nacional de Registro de Identificação Civil (CANRIC) e ABIS (do inglês *Automated Biometric Identification System*), respectivamente. A previsão desse novo modelo sustenta a não duplicação de registros e a consequente identificação unívoca dos cidadãos brasileiros natos e naturalizados. O Programa RIC, portanto, visa otimizar o sistema de identificação e individualização do cidadão brasileiro nato e naturalizado com vistas a um perfeito funcionamento da gestão de dados da sociedade, agregando valor à cidadania, à gestão administrativa, à simplificação do acesso aos serviços disponíveis ao cidadão e à segurança pública do país.

Nesse contexto, o termo de cooperação entre MJ/SE e FUB/CDT define um projeto que objetiva identificar, mapear e desenvolver parte dos processos e da infraestrutura tecnológica necessária para viabilizar a implantação do número único de Registro de

Identidade Civil – RIC no Brasil.

O presente relatório tem como objetivo analisar o movimento referente à segurança jurídica e aos marcos regulatórios para a proteção de dados pessoais, efetuando, para tanto, levantamento da legislação brasileira que regulamenta o acesso e a cessão de dados pessoais constantes em banco de dados, assim como, a realização de um estudo comparado.

A importância do presente estudo destaca-se pela: (i) maciça utilização na internet de dados de natureza pessoal e (ii) o avanço tecnológico que torna quase onipresente a utilização da Internet.

2. VIDA PRIVADA, INTIMIDADE E BANCO DE DADOS

Questão primordial ao presente trabalho é entender claramente o que se está tutelando quando se fala em proteção de dados pessoais, motivo pelo qual separamos o presente capítulo em tópicos tratando dos institutos da privacidade, intimidade e banco de dados, adentrando ao final na questão dos denominados dados sensíveis.

2.1 Vida Privada e intimidade.

Dentre os Direitos personalíssimos encontram-se o direito à intimidade e o direito à privacidade[1] (CF/88, art. 5º, inciso X), *in verbis*:

> Art. 5º, inciso X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

Ambos constituem direitos da personalidade, mas não se pode confundi-los. Para o Professor Ferraz Junior (1993,p. 442), no âmago da privacidade se esconde a intimidade, sendo está o mais exclusivo dos direitos da privacidade, por não envolver direito de terceiros. Também o direito ao nome, à imagem, à reputação compõe o campo da privacidade. Contudo, a imagem, a reputação, o nome, ao contrário da intimidade, são

[1] O direito à privacidade tem raízes modernas. No antigo direito romano, a oposição entre o público e o privado tinha a ver com a separação entre o que era de utilidade comum (ambiente político) e o que dizia respeito à utilidade dos particulares (ambiente familiar). Contudo, essa oposição perde nitidez na era moderna, tendo em vista o surgimento da noção do social, comum tanto ao público (político) como ao privado (familiar) (FERRAZ JUNIOR, p. 441).

exclusivos (próprios), mas perante os outros. Ninguém tem um nome, uma imagem, uma reputação só para si mesmo, mas como condição de comunicação, diálogo e convívio perante o outro.

Segue-se daí que o princípio da exclusividade, que rege o direito à privacidade, aplica-se diferentemente aos seus objetos específicos. Assim, o inciso X do art. 5º da Constituição, ao tornar invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegura-lhes o domínio exclusivo em vários sentidos. A intimidade é o âmbito do exclusivo que alguém reserva para si, sem nenhuma repercussão social, nem mesmo ao alcance de sua vida privada que, por mais isolada que seja, é sempre um viver entre os outros (na família, no trabalho, no lazer em comum dentre outros) (FERRAZ JUNIOR, 1993, p. 442).

Não há um conceito absoluto de intimidade, embora se possa dizer que a sua premissa é o “estar sozinho”, sem excluir o segredo e a autonomia. A intimidade, então, pode ser conceituada como o modo de ser de determinado indivíduo, consistindo fundamentalmente na exclusão do conhecimento pelos demais daquilo que somente a ele diz respeito. Corresponde, então, a todos os fatos, informações, acontecimentos ou eventos que a pessoa deseje manter em seu foro íntimo.

Já a vida privada envolve a proteção de formas exclusivas de convivência. Trata-se de situações em que a comunicação é necessária. A vida privada pode envolver situações de opção pessoal (como a escolha do regime de bens no casamento), mas que, em certos momentos, requer a comunicação a terceiros (na aquisição de um imóvel, por exemplo). Por aí ela difere da intimidade, que não experimenta esta forma de repercussão. Diante de tais características tem-se que o direito à privacidade consiste em tutela indispensável ao exercício da cidadania e torna-se essencial para garantir o equilíbrio de poderes entre o cidadão e o Estado; entre o indivíduo e as corporações (TEPEDINO, 2004, p. 303-305).

A privacidade tem por conteúdo a faculdade de constranger os outros de informações que dizem respeito somente ao indivíduo, e ele deseja manter para si ao abrigo de sua única e discricionária decisão se expõe ou não determinada informação (FERRAZ JUNIOR, 1993, p. 440).

O respeito e a importância à identidade do indivíduo garantem o direito de não violação dos dados pessoais e biológicos. Os dados pessoais são, inclusive, passíveis de consulta e retificação pelo instituto do *Habeas Data*, consagrado pela Constituição em seu artigo 5º, inciso LXXII.

Ademais, o art. 12 da Declaração Universal dos Direitos do Homem, de 1948, em que se lê: "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda pessoa tem direito à proteção da lei".

Assim, tem-se que os direitos da personalidade são considerados imprescindíveis e essenciais por funcionarem como conteúdo mínimo da personalidade humana e pode ser definido como uma categoria especial de direitos subjetivos que, fundada na dignidade humana, garantem o gozo e o respeito ao seu próprio ser, em todas as suas manifestações.

Pietro Perlingieri (2002, p. 38) salienta que a tutela da personalidade não é orientada apenas aos direitos individuais pertencentes ao indivíduo no seu precípuo e exclusivo interesse, mas, sim, aos direitos individuais sociais. Eles não devem ser entendidos como pertencentes ao indivíduo fora da comunidade na qual vive, mas, antes, como instrumentos para construir uma comunidade.

Perlingieri (2002, p.155-156) ainda destaca que a tutela da personalidade não se encerra na postulação de uma série, finita ou não, de direitos subjetivos, nem em um único direito subjetivo com auspícios de generalidade. A personalidade visa à proteção direta da pessoa, que é o valor máximo do ordenamento e sua proteção apenas através do mecanismo do direito subjetivo, um instituto forjado para se adequar às relações jurídicas patrimoniais, se mostra inadequado.

2.2 Dados Sensíveis

A informação pessoal pode estruturar-se em subcategorias, ligadas a determinado aspecto da vida de um indivíduo. Por exemplo, aplicam-se diretamente às informações referentes a movimentações bancárias de uma pessoa, o sigilo bancário. Esta setorização pode servir a escopos diferentes, desde uma fragmentação da tutela – que se estruturaria em torno de contextos setoriais, e não da pessoa – ou então, dentro de um panorama de tutela integral da pessoa, para mera especificação da abordagem a ser dada.[2]

Neste último sentido, a prática do direito da informação deu origem à criação de uma categoria específica de dados, os chamados dados sensíveis. Estes seriam determinados

[2] Brasil. A proteção de dados pessoais nas relações de consumo: para além da informação creditícia. Escola Nacional de Defesa do Consumidor – ENDC. Disponível em: http://www.vidaedinheiro.gov.br/docs/Caderno_ProtecaoDadosPessoais.pdf. Acesso em 01/11/2014.

tipos de informação que, se conhecidas e processadas, prestar-se-iam a uma potencial utilização discriminatória ou lesiva, particularmente mais intensa e que apresentaria maiores riscos potenciais que a média.[3]

Um dos conceitos utilizados para dados sensíveis é aquele apresentado pelo Tribunal Europeu de Direitos Humanos - TEDH, segundo o qual seria qualquer informação relativa a um indivíduo identificado ou identificável. Os dados protegidos pelo direito não se restringem àqueles concernentes a vida privada do indivíduo, mas também aos próprios fatos e acontecimentos referentes à sua vida pública, desde que afetem o desenvolvimento de sua personalidade (RUARO e RODRIGUEZ, 2010, p. 171-172).

De acordo com o entendimento do TEDH, o conteúdo e os limites do direito à proteção de dados passou a depender justamente da sua análise no caso concreto, tanto pela natureza do dado quanto pela forma como foi utilizado.

Assim, a própria seleção de quais seriam tais dados provém da avaliação de que a circulação de determinadas espécies de informação apresentaria um elevado potencial lesivo aos seus titulares.

Diante desse posicionamento (reconhecimento ou não do direito à proteção de dados deve levar em conta a sua natureza específica) o TEDH passou a considerar alguns dados pessoais como dados sensíveis, os quais se caracterizam por afetarem mais diretamente o desenvolvimento da personalidade humana, como é o caso relativo à orientação sexual, estadias em orfanatos durante a infância, ideologias políticas e dados médicos.

Desta forma, mesmo dados não qualificados como sensíveis, quando submetidos a um determinado tratamento, podem revelar aspectos sobre a personalidade de alguém, podendo levar a práticas discriminatórias. Afirma-se, em síntese, que um dado, em si, não é perigoso ou discriminatório – mas o uso que dele se faz pode sê-lo.

Dessa forma, o Tribunal Europeu entendeu que, para tais dados, a proteção devida deveria ser muito mais forte do que a dada aos demais dados, devendo-se utilizar não apenas o princípio geral de confidencialidade, mas uma verdadeira barreira a qualquer forma de publicidade (RUARO e RODRIGUEZ, 2010, p. 171-172).

[3] Brasil. A proteção de dados pessoais nas relações de consumo: para além da informação creditícia. Escola Nacional de Defesa do Consumidor – ENDC. Disponível em: http://www.vidaedinheiro.gov.br/docs/Caderno_ProtecaoDadosPessoais.pdf. Acesso em 01/11/2014.

Destarte, a Diretiva 95/46/CE, de 1995, disciplinou que os Estados-membros da União Europeia estariam proibidos de utilizar, de qualquer maneira, dados pessoais que revelassem a origem racial ou étnica da pessoa tutelada, suas opiniões políticas, convicções religiosas ou filosóficas e filiação sindical, da mesma forma que vetou o tratamento de dados relativos à saúde ou à vida sexual do indivíduo. Esta proteção, entretanto, poderia ser afastada quando presentes alguns requisitos, como dispôs a mesma Diretiva, ou mesmo nos casos de consentimento explícito da pessoa tutelada. (RUARO e RODRIGUEZ, 2010, p. 172).

Outro problema é que a mera proibição da coleta e tratamento – recurso utilizado por algumas das leis sobre a matéria - demonstra-se inviável, pois ocasionalmente o uso de tais dados é legítimo e necessário; além do que existem determinados organismos cuja própria razão de ser estaria comprometida caso não pudessem obter informações deste gênero, como algumas entidades de caráter político, religioso ou filosófico. [4]

O tratamento de dados sensíveis é, portanto, possível e mesmo necessário em uma série de circunstâncias, porém deve ser sempre uma exceção justificada pela relevância dos valores em questão e verificado que não há possibilidade de que seja realizada uma utilização discriminatória dos dados.

Atualmente, no entanto, o próprio conceito de dados sensíveis como fator que fundamenta uma proteção de nível mais elevado tende a ceder à noção de tratamento sensível de dados pessoais. Esta tendência provém do reconhecimento de que não é possível, hoje, prenunciar as causas e efeitos que um tratamento de dados pessoais possa causar ao seu titular apenas a partir da consideração da natureza dos dados que são tratados.[5]

2.3 Banco de Dados

A agilidade com que a manipulação de informações pessoais, banco de dados, pode ser feita com os computadores dá origem a diversas situações. A utilização de cadastros de proteção ao crédito (SERASA e SPC) hoje em dia, por exemplo, é parte integrante da

[4] Brasil. A proteção de dados pessoais nas relações de consumo: para além da informação creditícia. Escola Nacional de Defesa do Consumidor – ENDC. Disponível em: http://www.vidaedinheiro.gov.br/docs/Caderno_ProtecaoDadosPessoais.pdf. Acesso em 01/11/2014.

[5] *Ibid.*

atividade comercial, seja na pesquisa de consumidores inadimplentes, seja no relacionamento com antigos e novos clientes, entre outras situações. A Administração pública por sua vez, necessita de informações pessoais para o melhor planejamento e implementação de políticas públicas. Ademais, salienta-se que a informação de dados cresce muito mais quando são utilizados os bancos de dados cruzados, ou seja, ao serem relacionadas informações de diversos banco de dados.[6]

Nesse novo panorama, a privacidade deixa de ser um meio de garantir o isolamento de alguns para cumprir também outra função, que é reagir contra políticas de discriminação baseadas em opiniões e opções religiosas, políticas e sexuais, bem como outras questões. Há uma tendência à identificação de sujeitos coletivos, minorias de diversas ordens, como os mais prejudicados por esta configuração de dano à privacidade.[7]

A grande dificuldade da sociedade moderna é encontrar meios efetivos de proteger a privacidade a partir do controle das informações pessoais. A difícil questão obriga a resposta preliminar de duas outras indagações: a primeira, quais as informações pessoais cuja manipulação seria potencialmente prejudicial e qual espécie de manipulação seria aceitável; e a segunda, além da investigação sobre quais as formas pelas quais o dano poderia ocorrer.[8]

A proteção da privacidade, elemento indissolúvel da personalidade, merece esta tutela integrada, sendo provavelmente um dos casos em que ela é mais necessária. A cotidiana redefinição de forças e meios que possibilitam a intromissão na esfera privada dos indivíduos demanda uma tutela de caráter incessantemente mutável.

Assim, a necessidade da proteção de dados pessoais faz com que a tutela da privacidade ganhe um novo eixo. Considerando-se a esfera privada como um conjunto de ações, comportamentos, preferências, opiniões e comportamentos pessoais sobre os quais o interessado deseja manter um controle exclusivo, esta tutela há de basear-se em um novo "direito à autodeterminação informativa", hoje possível de ser identificado em diversos ordenamentos, que estabelece condições para um efetivo controle das informações pessoais em circulação.

---

6 DONEDA, Danilo. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. P. 6

7 *Ibid.*

8 *Ibid.*

Havendo dano, seja a uma coletividade ou a indivíduos, o certo é que a proteção mais adequada para a privacidade não reside mais na garantia de isolamento e segredo, mas sim em uma perspectiva de amplo controle da circulação das informações pessoais. Pode-se considerar uma transformação na definição do direito à privacidade, do "direito a ser deixado em paz" para o "direito a controlar o uso que outros fazem das informações que me digam respeito". Danilo Doneda[9] sugere algumas premissas que devem nortear os bancos de dados:

> (I) não deve existir um sistema de armazenamento de informações pessoais cuja existência seja mantida em segredo;
> (II) deve existir um meio para um indivíduo descobrir quais informações a seu respeito estão contidas em um registro e de qual forma ela é utilizada;
> (III) deve existir um meio para um indivíduo evitar que a informação ao seu respeito colhida para um determinado fim seja utilizada ou disponibilizada para outros propósitos sem o seu conhecimento;
> (IV) deve existir um meio para um indivíduo corrigir ou retificar o registro de informações a seu respeito; e
> (V) toda organização que estruture, mantenha, utilize ou divulgue registros com dados pessoais deve garantir a confiabilidade destes dados para os fins pretendidos e deve tomar as devidas precauções para evitar o mau uso destes dados.

Diante das premissas supramencionadas surgem os seguintes princípios[10].

> A) Princípio da transparência: o tratamento de dados pessoais não pode ser realizado sem o conhecimento do titular dos dados, que deve ser informado especificamente sobre todas as informações relevantes concernentes a este tratamento.
> B) Princípio da qualidade: os dados armazenados devem ser fidedignos à realidade, atualizados, completos e relevantes, o que compreende a necessidade de que sua coleta e seu tratamento sejam feitos com cuidado e correção, e de que sejam realizadas atualizações periódicas.
> C) Princípio da finalidade: qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados. Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da

9 DONEDA, Danilo. *Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade*. Disponível em: < http://www.estig.ipbeja.pt/~ac_direito/Consideracoes.pdf>. Acesso em 05/11/2014.

10 Brasil. A proteção de dados pessoais nas relações de consumo: para além da informação creditícia. Escola Nacional de Defesa do Consumidor – ENDC. Disponível em: http://www.vidaedinheiro.gov.br/docs/Caderno_ProtecaoDadosPessoais.pdf. Acesso em 01/11/2014.

transferência de dados pessoais a terceiros, além do que pode-se, a partir dele, estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade (fora da qual haveria abusividade).

D) Princípio do livre acesso: o indivíduo deve ter acesso às suas informações armazenadas em um banco de dados, podendo obter cópias destes registros. Por meio deste acesso as informações incorretas poderão ser corrigidas (atendendo com isso o princípio da qualidade), canceladas, suprimidas, ou mesmo acrescidas.

E) Princípio da segurança física e lógica: os dados devem ser protegidos por meios técnicos e administrativos adequados contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado.

Frisa-se, por oportuno, que há diversas modificações e adaptações destes princípios, quase sempre a partir deste mesmo núcleo comum. Não obstante, em alguns países, a tutela autônoma dos dados pessoais foi um primeiro passo rumo à sua consideração como um direito fundamental, em especial os integrantes da União Europeia.

3. PROTEÇÃO DE DADOS NO BRASIL – LINHA HISTÓRICA

O Brasil ainda não dispõe de proteção adequada e específica para dados de natureza pessoal. As principais legislações sobre o tema são:

a) Constituição Federal/1988 – Artigo 1º, III, artigo 5º, incisos IV, XII, XIV, XXXIII, XXXIV, aliena b), XXXIX, LV, LXXII e LXXVII;
b) Código Civil (CC) – Artigo 1º e artigo 21, 186,187, 188 e 927;
c) Código de Defesa do Consumidor (CDC) – Artigos 43, 72 e 73; e
d) Lei de Acesso à Informação (Lei n.º 12.527/11).

O ordenamento jurídico brasileiro passou a preocupar-se com o assunto recentemente, por meio da Constituição de 1988, a qual estabelece em seu artigo 5º um rol não exaustivo de direitos fundamentais garantidos a todo cidadão. Entre eles encontram-se diversos provimentos sobre privacidade e sobre proteção de dados, como a inviolabilidade das comunicações e o direito ao *habeas data*[11] no inciso LXXII.

Dispõe o inciso X do referido artigo da Constituição Federal/88 que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". Essa proteção geral dada no âmbito da privacidade é alvo de diversas interpretações e não se trata de um texto específico sobre a proteção de dados.

Ademais, a CF/88, no art. 5º, inciso IV, esclarece que "é livre a manifestação do pensamento, sendo vedado o anonimato". O inciso XII do mesmo artigo, determina a inviolabilidade do sigilo de comunicações, de dados e comunicações telefônicas, salvo por ordem judicial para fins de investigação criminal e instrução processual penal.

O Código Civil em seu Art. 21 estabelece que o judiciário, a pedido do ofendido, pode adotar providências para cessar as ofensas, uma vez que "a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma".

[11] O habeas data pode enquadra-se nos meios subjetivos de controle dos dados pessoais, através de impulso do interessado. Ele destina-se à obtenção e eventual retificação das informações sobre o impetrante em bancos de dados governamentais ou de caráter público.

O Código de Defesa do Consumidor (CDC) já explicita uma proteção extensa a dados relativos às relações de consumo. A Seção VI do Capítulo V do Título I do CDC trata especificamente sobre bancos de dados e cadastro de consumidores garantindo, no seu Art. 43, que "o consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes". O mesmo artigo garante em seus parágrafos 2º e 3º, respectivamente, que "a abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele" e que "o consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção (...)".

O Art. 43, § 4º, do CDC considera os bancos de dados de consumidores algo de caráter público. Desta forma, em uma interpretação integrativa da lei, o acesso aos bancos de dados de registros pessoais das relações de consumo é igualmente assegurado por meio de *habeas data*.

Ademais, o CDC estabeleceu para o consumidor o direito de acesso e retificação de informações suas que sejam armazenadas por fornecedores, além da vedação da manutenção deste registro por mais de 5 anos.[12]

A Lei de acesso à informação (Lei n.º 12.527/11) trouxe em seu artigo 10º a prerrogativa de qualquer interessado apresentar "pedido de acesso à informação" aos órgãos e entidades, buscando com isso dar transparência às informações públicas, regulando a determinação contida no inciso XXXIII do art. 5º, no inciso II do §3º do art. 37 e no §2º do art. 216 da Constituição Federal.

Destaca-se ainda o art. 3º, §2º da Lei n.º 7.232/84, sobre a Política Nacional de Informática, dispondo que "a estruturação e a exploração de bancos de dados serão regulados por lei específica", o que ainda não foi feito.[13]

As primeiras discussões sobre a confecção de uma Lei própria se deram nos subgrupos de Trabalho (SGTs), criados na estrutura institucional do MERCOSUL, na qual se discutia

[12] DONEDA, Danilo. *Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade*. Disponível em: < http://www.estig.ipbeja.pt/~ac_direito/Consideracoes.pdf>. Acesso em 05/11/2014

[13] Seus contornos foram definidos pela sua regulamentação, na Lei 9.507/97. Algumas de suas limitações, porém, fazem com que sua aplicação seja escassa e pouco abrangente, como a exclusão de bancos de dados privados e de uso interno do seu campo de atuação; a necessidade da prova da recusa da administração (ou outro ente) em fornecer a informação; e a ausência da possibilidade expressa de que informações indevidamente coletadas ou armazenadas sejam eliminadas do banco de dados.

a necessidade do Brasil incrementar seu arcabouço jurídico relacionado à proteção de dados pessoais, sobretudo a fim de obter uma validação internacional acerca do nível adequado de proteção dos dados pessoais. A primeira discussão organizada se deu em um Seminário Internacional de Proteção de Dados Pessoais ocorrido em novembro de 2005, que teve o objetivo de discutir os modelos jurídicos existentes nos países da Europa e América Latina, e qual seria mais adequado à realidade brasileira.[14]

A discussão ficou paralisada até 2010, quando o Governo Brasileiro, por meio do Ministério da Justiça, elaborou um Anteprojeto de Lei de Proteção de Dados Pessoais (ALPDP) para regulamentação do tema, colocando para Consulta Pública na Internet. Entre 2011 e 2013 o anteprojeto de lei em referência passou por análise de diversos órgãos e entidades, o que acarretou em alterações no seu texto.

Paralelamente, caminhou o Projeto de Lei n.º 4.060/2012, que dispõe sobre o tratamento de dados pessoais e outras providências com objetivo de resguardar os anseios do setor de comunicação e *marketing*, bem como a defesa dos consumidores.

Em 20 de maio de 2014, o Senador Vital do Rêgo apresentou o projeto de Lei do Senado n.º 181/2014, que pretende disciplinar a atividade de tratamento de dados pessoais realizada no território brasileiro ou que nele se possa produzir efeitos. A proposta apresenta 19 artigos reproduzidos a seguir, contendo os seguintes destaques:

> Capítulo I
> Do Objeto e Âmbito de Aplicação
> Art. 1º **Esta Lei regula a proteção, o tratamento e o uso de dados das pessoas naturais e <u>jurídicas</u>** de direito público ou privado.
> Parágrafo único. Reger-se-á por esta Lei todo tratamento de dados pessoais, qualquer que seja o mecanismo empregado, quando sua coleta, armazenamento ou utilização ocorrer em território nacional ou em local onde seja aplicável a lei brasileira, por força de tratado ou convenção.
> Art. 2º A presente Lei não se aplica ao tratamento de dados efetuado por pessoa física na consecução de suas necessidades privadas.
> Capítulo II
> **Das Definições**
> Art. 3º Para os efeitos desta Lei, considera-se:
> **I – dado pessoal: toda informação, de qualquer natureza e independentemente do respectivo suporte, passível de ser armazenada, processada ou transmitida, relativa a pessoas identificadas ou identificáveis;**

[14] ABEMD. *Proteção de Dados no Brasil – Linha do Tempo*. Disponível em: <http://abemd.org.br/interno/cafe_030914_protecao_de_dados.pdf>. Acesso em 25/11/2014.

II – banco de dados: conjunto estruturado de dados pessoais, centralizado ou descentralizado de modo funcional ou geográfico, acessível segundo critérios determinados, qualquer que seja a forma de gerenciamento;
III – tratamento de dados pessoais: qualquer operação ou conjunto de operações, em um ou mais bancos de dados, independentemente do mecanismo utilizado;
IV – gestor de banco de dados: a pessoa física ou jurídica, de direito público ou privado, constituída sob qualquer forma, que, individual ou coletivamente, determine as finalidades, os meios de tratamento e a utilização dos dados pessoais;
V – gestor aparente: a pessoa física ou jurídica, de direito público ou privado, responsável, por delegação do gestor de banco de dados, pelo tratamento dos dados pessoais;
VI – proprietário do banco de dados: a pessoa física ou jurídica, de direito público ou privado, proprietária dos meios físicos e eletrônicos constituintes do banco de dados e detentora das informações objeto de tratamento pelo banco de dados;
VII – titular de dados pessoais: a pessoa natural ou jurídica, de direito público ou privado, a que se referem as informações coletadas, armazenadas, processadas ou transmitidas;
VIII – usuário de banco de dados: a pessoa física ou jurídica, de direito público ou privado, que acessa e utiliza as informações tratadas pelo banco de dados, mediante requerimento ou por força de disposição legal;
IX – **dados sensíveis**: informações pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas, ideológicas ou filosóficas, a filiação e atuação sindical, o estado de saúde ou a orientação sexual da pessoa natural titular dos dados, bem como as informações genéticas;
X – interconexão de dados: forma de tratamento de informações pessoais que consiste na transferência de dados de um banco a outro, mantido ou não pelo mesmo proprietário, com finalidade semelhante ou distinta;
XII – dissociação: procedimento destinado a impedir a identificação da pessoa a que se refere a informação coletada, armazenada ou transmitida.
§ 1º Considera-se identificável a pessoa passível de reconhecimento, direta ou indiretamente, mediante referência a um número de identificação ou a um ou mais elementos específicos de sua identidade física, fisiológica, psíquica, econômica, cultural ou social.
§ 2º Para os fins do disposto no inciso III deste artigo, configuram tratamento de dados pessoais a pesquisa, o recolhimento, o registro, a organização, a classificação, a comparação, a valoração, a conservação, a modificação, a adaptação, a alteração, a recuperação, a consulta, a utilização, a transferência, a transmissão, por difusão ou por qualquer outra forma de comunicação, a interconexão, o bloqueio, o descarte e a destruição da informação.
§ 3º Para os fins do disposto nos incisos IV e V deste artigo, **consideram-se gestores de bancos de dados, ou gestores aparentes, por equiparação, o serviço instituído com a mesma finalidade, ainda que desprovido de personalidade jurídica, e os órgãos da administração pública direta.**
§ 4º As finalidades e os meios de tratamento dos dados pessoais, quando se tratar de banco de dados de titularidade de pessoa jurídica

de direito público, serão exercidos em atenção às atribuições e competências legais e institucionais do titular.
§ 5º Para efeito do que dispõe o inciso VIII deste artigo, incluem-se na definição de usuário de bancos de dados os órgãos da administração direta de quaisquer esferas de governo.
§ 6º Considera-se privativo o uso das informações armazenadas no âmbito de organizações, públicas ou privadas, respeitadas as finalidades para as quais foi criado o banco de dados e observados os princípios definidos nesta Lei.
Capítulo III
Do Tratamento de Dados Pessoais
Art. 4º Ao tratamento de dados pessoais aplicam-se os seguintes **princípios**:
I – coleta, armazenamento e processamento de forma lícita, com observância do princípio da boa-fé e adstritos a finalidades determinadas, vedada a utilização posterior incompatível com essas finalidades;
II – adequação, pertinência, exatidão e atualização, periódica e de ofício, das informações;
III – conservação dos dados e identificação dos seus titulares apenas pelo período necessário às finalidades da coleta ou tratamento;
IV – consentimento prévio e expresso do titular de dados como requisito à coleta, quando se tratar de dados sensíveis ou de interconexão internacional de dados realizada por banco de dados privado (art. 10);
V – prévia ciência do titular das informações, quando se tratar de dados para os quais o consentimento expresso é inexigível;
VI – acesso do titular de dados às informações coletadas, armazenadas, processadas ou transmitidas.
§ 1º Excetua-se do disposto no inciso III a conservação de dados por órgãos e pessoas jurídicas de direito público ou realizada para fins históricos, estatísticos e científicos.
§ 2º Incumbe ao gestor de banco de dados zelar pela observância do disposto neste artigo, especialmente pela adequação e pertinência das informações tratadas, com a devida retificação ou cancelamento de dados inexatos, incompletos ou que deixarem de ser necessários à finalidade para a qual foram coletados.
Art. 5º Os dados considerados sensíveis somente poderão ser coletados, armazenados, processados, transmitidos, utilizados, fornecidos a usuários ou divulgados:
I – com o expresso, específico e inequívoco consentimento de seu titular ou representante legal;
II – para fins meramente estatísticos, históricos ou científicos, vedada a identificação do titular;
III – por força de decisão judicial;
IV – por expressa disposição legal;
V – por relevante interesse público, na forma do regulamento desta Lei;
VI – com o objetivo de preservar o direito à vida do titular de dados.
§ 1º O consentimento previsto no inciso I deste artigo não se aplica aos dados sensíveis tornados públicos por seu titular, como resultado inequívoco de sua manifestação de vontade.
§ 2º Sem prejuízo do disposto no inciso V deste artigo, considera-se de relevante interesse público o tratamento de dados realizado para fins de medicina preventiva, de diagnóstico ou tratamento médico, ou gestão de

serviços de saúde, desde que efetuado por pessoa obrigada a sigilo profissional.
§ 3º O tratamento de dados sensíveis fundado em relevante interesse público somente poderá ocorrer por órgãos da administração pública direta, pessoas jurídicas de direito público ou pessoas jurídicas de direito privado no exercício da medicina ou proteção à saúde, observadas suas funções institucionais.
§ 4º O disposto no inciso VI deste artigo somente se aplica quando impossível a obtenção do consentimento do titular de dados ou da autorização de seu representante legal.
Art. 6º O tratamento de dados pessoais para fins de segurança pública, investigação criminal ou instrução penal, administrativa ou tributária somente poderá ser feito por órgão da administração pública direta ou pessoa jurídica de direito público, limitando-se às seguintes hipóteses:
I – exercício de competência prevista em lei;
II – prevenção ou repressão de infração penal, administrativa ou tributária;
III – compartilhamento de informações para fins de segurança do Estado e da sociedade;
IV – atendimento dos termos de acordo, tratado ou convenção internacional de que o Estado brasileiro seja parte.
Capítulo IV
Dos Direitos Básicos do Titular de Dados
Art. 7º São direitos básicos do titular de dados:
I – o respeito às liberdades e garantias fundamentais da pessoa humana, em especial à inviolabilidade de consciência e de crença e à proteção da vida privada, intimidade, honra e imagem;
II – o acesso à origem e ao conteúdo de dados pessoais coletados e tratados em banco de dados;
III – a ciência prévia, e por escrito, como requisito à inclusão de informações pessoais em banco de dados;
IV – a retificação, a título gratuito, de dados pessoais inexatos, incompletos, omissos, inverídicos ou desatualizados;
V – o consentimento prévio como requisito à coleta e ao tratamento de dados pessoais sensíveis, bem como à interconexão internacional de dados realizada por banco de dados privado (art. 10);
VI – o cancelamento, a título gratuito, de dados que deixarem de ser necessários à consecução da finalidade para a qual foram coletados;
VII – a oposição, a título gratuito, à inclusão, cessão ou transmissão de informações pessoais que tenham por finalidade a publicidade ou divulgação comercial;
VIII – a exclusão ou a dissociação gratuitas de dados pessoais sensíveis inseridos em banco de dados, se manifesto o interesse;
IX – a exclusão automática, após o prazo de cinco anos, a contar da inscrição, de dados pessoais capazes de gerar restrições à obtenção de crédito;
X – a facilitação da defesa de seus direitos em processos judiciais ou administrativos, admitida a inversão do ônus da prova, quando, a critério do juiz, for verossímil a alegação.
§ 1º Ao direito de acesso previsto no inciso II do caput deste artigo aplicam-se as seguintes regras:
I – poderá ser exercido a qualquer tempo, mediante solicitação escrita dirigida ao gestor ou ao proprietário do banco de dados;

II – será gratuito, quando não exercido por mais de uma vez no período de doze meses;
III – será deferido ou indeferido no prazo de quarenta e oito horas e a decisão comunicada ao requerente em vinte e quatro horas.
§ 2º A ciência prévia a que se refere o inciso III deste artigo:
I – constitui requisito necessário à inclusão da informação no banco de dados;
II – é inexigível quando o banco de dados for mantido por órgão da administração pública direta ou pessoa jurídica de direito público, ou quando a informação tenha sido coletada diretamente do titular dos dados;
III – pode ser dispensada se o tratamento não identificar o titular de dados e possuir fins meramente históricos, estatísticos ou científicos.
§ 3º Poderá ser requerido o cancelamento de informação não sensível quando o banco de dados lhe houver atribuído finalidade diversa daquela para a qual foi coletada.
§ 4º À pessoa jurídica titular de dados são reconhecidos os direitos compatíveis com sua natureza
Capítulo V
Do Proprietário e do Gestor de Banco de Dados
Art. 8º Constituem deveres do proprietário e do gestor de banco de dados, no tratamento de dados pessoais:
I – informar aos titulares de dados pessoais:
a) a inclusão e o tratamento de suas informações;
b) a extensão de seus direitos;
c) a finalidade da coleta;
d) as categorias de usuários da informação;
e) a identidade do proprietário e do gestor do banco de dados;
II – não utilizar os dados para finalidades incompatíveis com aquelas para as quais foram coletados;
III – não proceder a tratamento de dados por meios fraudulentos, desleais ou ilícitos;
IV – não utilizar os dados com a finalidade exclusiva de revelar a terceiros a origem racial ou étnica, crença religiosa, filosófica, política ou ideológica, atuação partidária ou sindical, estado de saúde, informações genéticas ou orientação sexual da pessoa natural do titular dos dados;
V – oferecer proteção e segurança aos dados coletados, observada a natureza destes e os riscos a que estejam expostos, a fim de impedir sua perda, destruição, alteração, tratamento, cópia, difusão ou acesso não autorizado;
VI – não inserir dados oriundos de fontes acessíveis ao público sem que prévia ciência seja conferida ao titular dos dados;
VII – não inserir dados pessoais sensíveis sem o consentimento prévio e expresso do titular dos dados;
VIII – apreciar, no prazo máximo de dez dias, a contar da solicitação, pedido de retificação, oposição, cancelamento e exclusão de dados;
IX – retificar, independentemente de provocação do titular, dados inexatos, incompletos, inverídicos ou desatualizados;
X – cancelar, independentemente de provocação do titular, dados que deixarem de ser necessários à consecução da finalidade para a qual foram coletados;
XI – indenizar, por danos morais e materiais, os titulares de dados coletados, tratados ou utilizados em desacordo com as prescrições legais,

sem prejuízo da responsabilidade administrativa ou penal que lhes possa ser imputada.

Parágrafo único. O dever de sigilo relativo ao tratamento de dados sensíveis estende-se a todas as pessoas que tenham acesso às informações por vínculo contratual com o proprietário ou o gestor do banco de dados, subsistindo mesmo após o encerramento da relação jurídica.

Capítulo VI

Disposições Especiais Aplicáveis aos Bancos de Dados Públicos

Art. 9º **Considera-se público o banco de dados cujo proprietário seja órgão da administração pública direta, pessoa jurídica de direito público ou pessoa jurídica de direito privado no exercício de serviço público ou função delegada pelo Poder Público**.

§ 1º Ao banco de dados público que tenha por objeto tratamento de dados com vistas a auxiliar atividade de segurança nacional ou pública, investigação administrativa, tributária, criminal ou instrução processual penal, não se aplica o disposto nos incisos II, III, IV, V, VI e VIII do caput do art. 7º e nos incisos I, VI, VII e VIII do art. 8º, sem prejuízo da responsabilidade civil ou penal que ao titular ou gestor possa ser imputada por desvio de finalidade no uso das informações tratadas.

§ 2º O disposto nos incisos III e V do caput do art. 7º e nos incisos VI e VII do art. 8º não se aplica ao banco de dados público que tenha por objeto tratamento de dados pessoais necessários à prevenção e ao diagnóstico médico ou à vigilância sanitária, sem prejuízo da responsabilidade civil ou penal que ao titular ou gestor possa ser imputada por desvio de finalidade no uso dos dados.

§ 3º O banco de dados público que tenha por objeto tratar dados pertencentes a grupos de profissionais não poderá utilizar os dados colhidos para finalidade diversa daquela a que se destinam, salvo consentimento expresso e prévio do titular de dados.

§ 4º O proprietário ou gestor de banco de dados público não poderá utilizar os dados tratados para fins de publicidade ou divulgação comercial.

Capítulo VII

Disposições Especiais Aplicáveis aos Bancos de Dados Privados

Art. 10. Considera-se privado o banco de dados cujo proprietário seja pessoa jurídica de direito privado no exercício de atividade privada, econômica ou não. § 1º Ao banco de dados privado que tenha por objeto tratar dados necessários à salvaguarda de interesse vital do titular não se aplica, quanto aos dados pessoais sensíveis sobre o estado de saúde, o disposto na primeira parte do inciso V do caput do art. 7º e no inciso VII do art. 8º, sem prejuízo da responsabilidade civil ou penal que ao titular ou gestor possa ser imputada por desvio de finalidade no uso dos dados.

§ 2º O banco de dados privado que tenha por objeto tratar dados pertencentes a grupos de profissionais não poderá utilizar os dados colhidos para finalidade diversa da que se destinam, salvo consentimento expresso e prévio do titular de dados.

§ 3º O proprietário ou gestor de banco de dados privado poderá utilizar os dados tratados, excetuados os dados sensíveis, para fins de publicidade ou divulgação comercial, mediante consentimento prévio conferido ao titular, o qual poderá exercer direito de oposição, nos termos do inciso VII do caput do art. 7º.

§ 4º Ao banco de dados privado que tenha por objeto tratar dados relativos à solvência patrimonial e de crédito aplicam-se as seguintes disposições:
I – inclusão de dados restritivos ao crédito somente após a ciência prévia do titular, mediante notificação por carta enviada para o domicílio deste;
II – exclusão automática dos dados incluídos há mais de cinco anos, sem prejuízo dos demais direitos atribuíveis ao titular das informações, nos termos dos arts. 6º e 7º e das normas que regulam as relações de consumo.
§ 5º Para efeito do disposto no § 4º, inciso I, deste artigo, poderá o banco de dados promover o registro sem proceder à ciência prévia se o titular não possuir domicílio certo ou conhecido, responsabilizando-se solidariamente com o solicitante pela veracidade desta informação.
Capítulo VIII
Da Segurança dos Dados
Art. 11. Os proprietários e gestores de bancos de dados devem adotar, entre outras, as seguintes medidas destinadas à proteção dos dados pessoais contra a perda ou destruição acidental ou ilícita, a alteração, a difusão e o acesso não autorizados:
I – impedir que pessoas não autorizadas tenham acesso aos equipamentos, instalações e suportes de tratamento de dados;
II – garantir que somente usuários tenham acesso aos dados transmitidos;
III – garantir a possibilidade de verificação periódica das alterações produzidas nos arquivos de dados.
Parágrafo único. Não se registrarão dados sensíveis em bancos de dados que não reúnam condições mínimas de segurança, conforme definido no regulamento desta Lei.
Capítulo IX
Da Interconexão de Dados
Art. 12. A interconexão de dados pessoais deve atender aos seguintes requisitos:
I – adequação às finalidades legais ou estatutárias e aos interesses legítimos dos proprietários e gestores de bancos de dados;
II – não discriminação ou violação de direitos, liberdades e garantias dos titulares de dados;
III – proteção dos dados por medidas de segurança capazes de evitar sua perda, destruição, reprodução, replicação, difusão e o acesso não autorizado a seu teor.
§ 1º A interconexão internacional de dados por banco público somente será permitida se houver tratado ou acordo internacional autorizativo de que seja parte a República Federativa do Brasil, ou promessa de reciprocidade, e tiver por objetivo coibir crime organizado transnacional, tráfico de seres humanos, crime de corrupção, terrorismo, financiamento ao terrorismo, narcotráfico, lavagem de dinheiro, extorsão mediante sequestro ou crimes contra o sistema financeiro nacional, atendidas as seguintes condições:
I – expressa solicitação de autoridade competente estrangeira;
II – existência de pedido fundado na necessidade de investigação policial, instrução ou persecução criminal;
III – segurança assumida pelo Estado ou organismo internacional destinatário de nível adequado de proteção dos dados e informações.
§ 2º A interconexão internacional de dados por bancos de dados privados deverá atender ao seguinte:
I – prévio consentimento do titular das informações, atendidas as disposições desta Lei, que poderá ser dispensado na hipótese de dados

transmitidos em razão de transferências bancárias ou de operações realizadas em bolsa de valores;
II – intermediação do Estado brasileiro, para interconexão de dados sensíveis.

Capítulo X

Da Retificação e do Cancelamento de Dados

Art. 13. O requerimento de retificação ou de cancelamento de dados pessoais deverá ser instruído, conforme o caso, com documentos que comprovem:
I – a inexatidão, incompletude, omissão, falsidade ou desatualização da informação;
II – a prescindibilidade da informação para a consecução da finalidade para a qual foi realizada a coleta.
§ 1º As retificações e os cancelamentos, que deverão ser processados no prazo máximo de dez dias, a contar da notificação do gestor do banco de dados, serão comunicados por qualquer meio hábil ao titular dos dados e, sempre que possível, aos usuários.
§ 2º Recusada a retificação ou o cancelamento, será averbada, no cadastro do titular, a informação sobre a existência do requerimento e sua recusa, assim bem como o motivo da recusa.
§ 3º A informação de que trata o § 2º deste artigo possui natureza complementar, devendo acompanhar, obrigatoriamente, todo tratamento e comunicação dos dados aos quais se refere.

Capítulo XI

Da Responsabilidade Civil

Art. 14. Qualquer pessoa que sofra prejuízo decorrente do tratamento irregular ou ilícito de dados possui direito à reparação dos danos, materiais e morais.
§ 1º A responsabilidade do proprietário, do usuário, do gestor e do gestor aparente de banco de dados, quando houver, independe da verificação de culpa.
§ 2º O tratamento de dados realizado de forma associativa ou por qualquer outra forma, ainda que informal, acarreta a responsabilidade solidária e direta de todos os agentes envolvidos.
§ 3º O disposto neste artigo não exclui outras hipóteses de responsabilidade revistas em lei.

Capítulo XII

Das Sanções Administrativas

Art. 15. As infrações às normas de proteção de dados pessoais ficam sujeitas às seguintes sanções administrativas, sem prejuízo das de natureza civil, penal e das definidas em normas específicas:
I – multa;
II – suspensão temporária de atividade;
III – intervenção administrativa;
IV – interdição, total ou parcial, da atividade exercida pelo proprietário ou gestor de banco de dados.
Parágrafo único. As sanções previstas neste artigo serão aplicadas pelas autoridades administrativas federal, estadual, do Distrito Federal ou municipal, no âmbito de suas atribuições, conforme disciplinadas em normas regulamentares.
Art. 16. As penas serão aplicadas pela administração pública, mediante processo administrativo em que se assegure a ampla defesa, admitida:
I – a cumulação de penas;

> II – a imposição cautelar das sanções previstas nos incisos I e II do art. 15.
> **Art. 17. A pena de multa, graduada de acordo com a gravidade da infração, será fixada entre os limites de mil a vinte mil reais.**
> Art. 18. A produção, manuseio, consulta, transmissão, tratamento, manutenção e guarda de dados ou informações sigilosas de interesse da segurança da sociedade e do Estado, no âmbito da administração pública federal, permanecerão regidos pela Lei nº 8.159, de 8 de janeiro de 1991, e pelo Decreto nº 4.553, de 27 de dezembro de 2002.
> Art. 19. Esta Lei entra em vigor na data de sua publicação.

Outros de Projetos de Lei sobre o tema e suas repercussões também estão em trâmite no Senado, são estes: (i) o Projeto de Lei do Senado n.º 330/2013, do Senador Antônio Carlos Valadares (PSB/SE), o qual dispõe sobre todo tratamento de dados pessoais, qualquer que seja o mecanismo empregado, quando sua coleta, armazenamento ou utilização ocorrer em território nacional ou em local onde seja aplicável a lei brasileira, por força de tratado ou convenção; (ii) o Projeto de Lei do Senado n.º 131/2014, apresentado como conclusão do Relatório n.º 1, de 2014, da Comissão Parlamentar de Inquérito da Espionagem, estabelece condições para o fornecimento de dados de cidadãos ou empresas brasileiras a autoridades ou tribunais estrangeiros.

Por fim, em relação ao tema da proteção ao tratamento de dados pessoais, convém ressaltar a aprovação do Marco Civil da Internet, Lei n.º 12.965/2014, que dispõe sobre o assunto e trouxe algumas novidades como:

> - a necessidade de previsão expressa e detalhamento, em contratos de prestação de serviços, do regime de proteção aos dados pessoais, aos registros de conexão e aos registros de acesso a aplicações de Internet, bem como a necessidade de consentimento "livre, expresso e informado" do titular para o fornecimento de dados a terceiros (art. 7º, VI e VII);
>
> - cláusula referente ao consentimento expresso sobre a coleta deverá estar em destaque (art. 7º IX);
>
> - direito à exclusão definitiva de dados que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes (art. 7º, Xº); a vedação, na provisão de conexão à internet, ao bloqueio, monitoramento, filtragem ou análise do conteúdo de pacotes de dados (art. 9º, § 3º);
>
> - vedação à provisão de conexão de guarda de registros de acesso a aplicações à internet (art. 14);
>
> - necessidade do provedor de aplicações de internet de manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses (art. 15); e

- necessidade do provedor de conexão à internet de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano (art. 13).

Há, portanto, Projeto de Lei (PLS) n.º 181/14 de iniciativa do legislativo e, texto do governo, anteprojeto supostamente pronto, parado há mais de 4 anos no Ministério da Justiça. Em 2 de dezembro de 2014 o PLS nº 181/14 foi levado para discussão no Senado, sendo alvo de várias críticas por especialistas que apontaram várias lacunas e imprecisões como a falta de clareza na definição do que são 'dados pessoais' – por exemplo, se o endereço IP entra (como proposto), não obstante a unanimidade de uma legislação para proteção de dados pessoais.[15]

Desta forma, o momento atual em relação à proteção de dados pessoais é de expectativa no tocante às propostas de legislações, bem como de adequação no que se refere às disposições já inseridas no ordenamento jurídico pátrio pelo Marco Civil da Internet, o qual entrou em vigor em 23 de junho de 2014. Atualmente aguarda-se a versão final do Projeto de Lei de Proteção de Dados Pessoais. Tais instâncias tomaram por base diversas leis já em vigência no âmbito internacional, tais como a Diretiva Europeia de Proteção de Dados Pessoais (EC 95/46).

[15] http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=38563&sid=4#.VIJM-jHF8ms

4. COMENTÁRIOS AO ANTEPROJETO DE LEI SOBRE A PROTEÇÃO DE DADOS PESSOAIS

O atual estágio tecnológico, o qual torna a utilização, por exemplo, da Internet algo quase onipresente, a qual para seu funcionamento tem por costume a utilização massiva de dados de natureza pessoal (muitos deles sensíveis, como cor, sexo e orientações políticas), enseja a imperatividade de um correto tratamento dessas informações.[16]

De fato, todos os dias os meios de comunicação veiculam notícias de vazamento de dados pessoais, cadastrais ou mesmo financeiros. Caio Cesar Carvalho Lima e Renato Leite Monteiro[17] relatam que uma compilação das chamadas *data breaches* (violação de dados), iniciada em 2005, revela que os vazamentos de dados já ultrapassam mais de três mil casos, ou aproximadamente 600 milhões de registros divulgados sem consentimento em países que já regulam a matéria relativa a estes incidentes.

O anteprojeto teve por base diversas leis já em vigência no âmbito internacional, tais como a Diretiva Europeia de Proteção de Dados Pessoais (95/46) e a Lei de proteção de dados canadense. A seguir elenca-se os principais artigos com comentários de Renato Leite Monteiro, Caio Cesar Carvalho Lima, Patrícia Peck Pinheiro e equipe.[18]

> 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, particularmente em relação à sua liberdade, igualdade e privacidade pessoal e familiar, nos termos do art. 5º, incisos X e XII da Constituição Federal.

Monteiro e Lima sugerem a inclusão do termo intimidade, em consonância com o artigo 5º da CF/88, bem como a expressa proteção econômica e consumerista.

Questão interessante é se o anteprojeto engloba tanto as pessoas físicas como as pessoas jurídicas. Patrícia Peck e equipe defendem que sim, tendo em vista que as pessoas jurídicas já gozam de direitos de proteção conforme artigo 5º, incisos X e XII da CF/88. Em

---

16 MONTEIRO, Renato Leite; LIMA, Caio César Carvalho. *Comentários ao Anteprojeto de Lei sobre Proteção de Dados Pessoais*. Disponível em: <http://securitybreaches.files.wordpress.com/2011/05/anteprojeto-de-lei-brasileiro-sobre-protecao-de-dados-pessoais.pdf>. Acesso em 11/11/2014.

17 MONTEIRO, Renato Leite; LIMA, Caio César Carvalho. *Panorama brasileiro sobre a proteção de dados pessoais: discussão e análise comparada*. Disponível em: http://www.atoz.ufpr.br/index.php/atoz/article/view/41/121. Acesso em 12/11/2014.

18 PECK, Patrícia. Parecer: *Contribuições para redação do anteprojeto de Lei. Proteção de Dados Pessoais*. Disponível em http://culturadigital.br/dadospessoais/files/2011/05/Patricia-Peck-Pinheiro-Advogados-Prote%C3%A7%C3%A3o-de-Dados.pdf. Acesso em 11/11/2014.

contrapartida, Monteiro e Lima defendem que já existem leis para proteção das pessoas jurídicas como as normas de Direito Concorrencial, a Lei de propriedade intelectual.

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

Monteiro e Lima defendem que o objetivo do anteprojeto é a proteção da pessoa física. Patrícia Peck e equipe, pelas mesmas razões do comentário do artigo 1º, sugerem inclusão do termo "pessoa natural".

> Art. 3º A presente lei aplica-se aos tratamentos de dados pessoais realizados no território nacional por pessoa física ou jurídica de direito público ou privado, ainda que o banco de dados seja localizado no exterior.
> § 1º A presente lei não se aplica:
> I – ao tratamento de dados pessoais realizado por pessoa física para fins exclusivamente pessoais e domésticos, desde que os dados tratados não sejam destinados à comunicação;
> II – aos bancos de dados utilizados para o exercício da atividade jornalística exclusivamente para tal fim.
> § 2º Os bancos de dados instituídos e mantidos para fins exclusivos de segurança pública, defesa, segurança do Estado e suas atividades de investigação e repressão de delitos serão regidos por legislação específica.

Monteiro e Lima salientam que a abrangência do artigo, incluindo banco de dados que se encontrem no exterior, condiz com a atual tendência tecnológica a exemplo das *Cloud Computing* (onde os dados podem ficar armazenados nos mais variados locais). Ademais, alertam para a importância da lei distinguir "banco de dados" de "base de dados".

> Art. 4º Para os fins da presente lei, entende-se como:
> I - dado pessoal: qualquer informação relativa a uma pessoa identificada ou identificável, direta ou indiretamente, incluindo todo endereço ou número de identificação de um terminal utilizado para conexão a uma rede de computadores;
> II - tratamento: toda operação ou conjunto de operações, realizadas com ou sem o auxílio de meios automatizados, que permita a coleta, armazenamento, ordenamento conservação, modificação, comparação, avaliação, organização, seleção, extração utilização, bloqueio e cancelamento de dados pessoais, bem como o seu fornecimento a terceiros por meio de transferência, comunicação ou interconexão;
> III - banco de dados: todo conjunto estruturado de dados pessoais, localizado em um ou vários locais, em meio eletrônico ou não;
> IV - dados sensíveis: dados pessoais cujo tratamento possa ensejar discriminação do titular, tais como aqueles que revelem a origem racial ou

étnica, as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação sindical, partidária o a organizações de caráter religioso, filosófico ou político, os referentes à saúde e vida sexual, bem como os dados genéticos e biométricos;
V - titular: pessoa física a quem se referem os dados pessoais que são objeto de tratamento nos termos desta lei;
VI - responsável: a pessoa física ou jurídica, de direito público ou privado, a que competem as decisões referentes às finalidades e modalidades de tratamento de dados pessoais;
VII - subcontratado: a pessoa jurídica contratada pelo responsável pelo banco de dados como encarregado do tratamento de dados pessoais;
VIII - comunicação: ato de revelar dados pessoais a um ou mais sujeitos determinados diversos do seu titular, sob qualquer forma;
IX - difusão: ato de revelar dados pessoais a um ou mais sujeitos indeterminados diversos do seu titular, sob qualquer forma;
X - interconexão: transferência de dados de um banco de dados a outro, mantido ou não pelo mesmo proprietário, com finalidade semelhante ou distinta;
XI - bloqueio: a conservação do dado pessoal ou do banco de dados com a suspensão temporária de qualquer operação de tratamento;
XII - cancelamento: a eliminação ou destruição de dados ou conjunto de dados armazenados em banco de dados, seja qual for o procedimento empregado;
XIII - dissociação: ato de modificar o dado pessoal de modo a que ele não possa ser associado, direta ou indiretamente, com um indivíduo identificado ou identificável;
XIV - dados anônimos: dados relativos a um titular que não possa ser identificado, nem pelo responsável pelo tratamento nem por qualquer outra pessoa, tendo em conta o conjunto de meios suscetíveis de serem razoavelmente utilizados pelo responsável pelo tratamento dos dados ou por qualquer outra pessoa para identificar o referido titular.

O artigo 4º conceitua diversos termos utilizadas na Lei em referência. Monteiro e Lima sugerem ainda inclusão de outros como do *opt-in* (anuência do indivíduo).

Art. 5º O tratamento de dados pessoais por parte de pessoas jurídicas de direito público é permitido para o cumprimento de suas funções institucionais, dentro dos limites da lei.

Art. 6º O tratamento de dados pessoais é atividade de risco e todo aquele que, por meio do tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, é obrigado a ressarci-lo, nos termos da lei.

Monteiro e Lima ponderam que o artigo sexto traz o instituto da responsabilidade objetiva das sociedades empresárias. Não obstante, ressalta-se discussão se o simples fato de sociedades empresárias exercerem atividade de risco ensejaria responsabilidade objetiva.

Art. 7º A defesa dos interesses e direitos dos titulares de dados poderá ser exercida em juízo individualmente ou a título coletivo, na forma do disposto nos artigos 81 e 82 da Lei 8.078, de 11 de setembro de 1990, na Lei 7.347 de 24 de julho de 1985 e nos demais instrumentos de tutela coletiva estabelecidos em Lei.

CAPÍTULO II
PRINCÍPIOS GERAIS DE PROTEÇÃO DE DADOS

Art. 8º Os responsáveis pelo tratamento de dados pessoais deverão atender, dentre outros, aos seguintes princípios gerais de proteção de dados pessoais:

I - Princípio da finalidade: a não utilização dos dados pessoais objeto de tratamento para finalidades distintas ou incompatíveis com aquelas que fundamentaram a sua coleta e que tenham sido informadas ao titular; bem como a limitação deste tratamento às finalidades determinadas, explícitas e legítimas do responsável;

II - Princípio da necessidade: a limitação da utilização de dados pessoais ao mínimo necessário, de forma a excluir o seu tratamento sempre que a finalidade que se procura atingir possa ser igualmente realizada com a utilização de dados anônimos ou com o recurso a meios que permitam a identificação do interessado somente em caso de necessidade;

III - Princípio do livre acesso: a possibilidade de consulta gratuita, pelo titular, de seus dados pessoais, bem como de suas modalidades de tratamento;

IV - Princípio da proporcionalidade: o tratamento de dados pessoais apenas nos casos em que houver relevância e pertinência em relação à finalidade para a qual foram coletados;

V - Princípio da qualidade dos dados: a exatidão dos dados pessoais objeto de tratamento, com atualização realizada segundo a periodicidade necessária para o cumprimento da finalidade de seu tratamento;

VI - Princípio da transparência: a informação ao titular sobre a realização do tratamento de seus dados pessoais, com indicação da sua finalidade, categorias de dados tratados, período de conservação destes e demais informações relevantes;

VII - Princípio da segurança física e lógica: o uso, pelo responsável pelo tratamento de dados, de medidas técnicas e administrativas proporcionais ao atual estado da tecnologia, à natureza dos dados e às características específicas do tratamento, constantemente atualizadas e aptas a proteger os dados pessoais sob sua responsabilidade da destruição, perda, alteração e difusão, acidentais ou ilícitas, ou do acesso não autorizado;

VIII - Princípio da boa-fé objetiva: o respeito à lealdade e à boa-fé objetiva no tratamento de dados pessoais;

IX - Princípio da responsabilidade: a reparação, nos termos da lei, dos danos causados aos titulares dos dados pessoais, sejam estes patrimoniais ou morais, individuais ou coletivos; e

X – Princípio da prevenção: o dever do responsável de, para além das disposições específicas desta Lei, adotar, sempre que possível, medidas capazes de prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

CAPÍTULO III
REQUISITOS PARA O TRATAMENTO DE DADOS PESSOAIS

> Art. 9º O tratamento de dados pessoais somente pode ocorrer após o consentimento livre, expresso e informado do titular, que poderá ser dado por escrito ou por outro meio que o certifique, após a notificação prévia ao titular das informações constantes no art. 11.
> § 1º Nos serviços de execução continuada, o consentimento deverá ser renovado periodicamente, nos termos do regulamento.
> § 2º O tratamento de dados pessoais de crianças somente será possível com o consentimento dos responsáveis legais e no seu melhor interesse, sendo vedada a utilização destes dados para finalidades comerciais.

Monteiro e Lima apontam o artigo 9º como sendo o ponto nerval da lei, ao tratar da aceitação expressa do titular dos dados pessoais. A norma em referência não discorre sobre a possibilidade de *opt-in* prévio por meio de mensagem não requisitada com o objetivo de conseguir a anuência para o tratamento dos dados. Segundo Monteiro e Lima alguns países já estabeleceram, inclusive, o *double opt-in*, como forma mais efetiva e proteção. Ademais, os referidos autores ainda sugerem diferenciar criança e adolescente para fins de consonância com o Estatuto da Criança e do Adolescente.

Patrícia Peck e equipe ressaltam que o parágrafo primeiro merece reparo, vez que o consentimento para o tratamento dos dados pessoais hoje possui limite inesgotável de tempo, não sendo necessária a renovação do consentimento previamente inferido. Ademais destacam que não seria coerente a necessidade de renovação de consentimento para serviços de execução continuada sempre que o contrato estiver em vigor. Nesta hipótese, Patrícia Peck sugere que seja estabelecido limite máximo de 5 anos, mantendo-se um raciocínio coeso no âmbito da economia, vez que é a necessidade de guarda padrão de documentos para fins fiscais.

> Art. 10. O consentimento pode ser revogado a qualquer momento

O art. 10 está em consonância com o art. 43 do CDC. Contudo, Patrícia Peck e equipe destacam que não existe forma ou exigência legal de como deve se dar essa manifestação.

> Art. 11. No momento da coleta de dados pessoais, o titular será informado de forma clara e explícita sobre:
> I - a finalidade para a qual os seus dados pessoais estão sendo coletados e de que forma serão tratados;
> II – a identidade e o domicílio do responsável pelo tratamento;

> III - a natureza obrigatória ou facultativa do fornecimento dos dados;
> IV - as consequências de uma eventual negativa em fornecê-los;
> V - os sujeitos para os quais os dados podem ser comunicados e o seu âmbito de difusão; e
> VI - os seus direitos, em particular da possibilidade de negar-se fornecer os dados pessoais e sobre o seu direito de acesso e retificação gratuitos.
> Parágrafo único. Considera-se nulo o consentimento prestado caso as referidas informações tenham conteúdo enganoso ou não tenham sido fornecidas de forma clara e explícita.

O artigo 11 trata dos requisitos para conseguir a anuência do titular dos dados pessoais, sob pena de nulidade na hipótese de informações tenham conteúdo enganoso ou não tenham sido fornecidas de forma clara e explícita.

> Art. 12. O consentimento, caso prestado em conjunto com outras declarações, deve figurar de forma expressa e apartada.
>
> Art. 13. O consentimento será dispensado quando o tratamento:
> I - for necessário para a execução de obrigações derivadas de um contrato do qual é parte o titular, para a execução de procedimentos pré-contratuais requeridos por este, ou para o cumprimento de uma obrigação legal por parte do responsável;
> II - referir-se a dados provenientes de registros, atos ou documentos públicos de acesso público irrestrito;
> III - for necessário para o exercício de funções próprias dos poderes do Estado;
> IV - for realizado unicamente com finalidades de pesquisa histórica, científica ou estatística;
> V - for necessário para a proteção da vida ou da incolumidade física do titular ou de um terceiro, nos casos em que o titular não possa prestar o próprio consentimento por impossibilidade física ou por incapacidade de compreensão;
> VI - for necessário para o exercício do direito de defesa ou para fazer valer um direito em sede judicial, desde que os dados coletados sejam tratados exclusivamente para esta finalidade e estritamente pelo período de tempo necessário para sua execução;
> VII - disser respeito a dados sobre o inadimplemento de obrigações por parte do titular, caso em que o titular deverá ser notificado previamente por escrito, nos termos do art. 43 da Lei nº 8.078/90 – Código de Defesa do Consumidor.

O art. 13 elenca os casos em que o consentimento será dispensado, dentre os quais os dados para fins estatísticos. Monteiro e Lima esclarecem que o setor de análise comportamental tem por base justamente dados estatísticos coletados de indivíduos que tiveram suas informações dissociadas. Chamada de *behavirol analysis* essa metodologia utiliza dados coletados durante a navegação de usuários em sítios virtuais. São obtidos por

meio de *cookies* ou mesmo registros de pesquisas, que permitem traçar perfis. Monteiro e Lima alertam que a análise estatística de comportamento virtual pode influenciar toda uma coletividade e atingir diretamente os hábitos de indivíduos, principalmente os comerciais.

> Art. 14. Os dados pessoais que forem objeto de tratamento deverão ser:
> I - tratados de forma lícita e com boa-fé;
> II - coletados e armazenados para finalidades determinadas, explícitas e legítimas;
> III – exatos, claros, objetivos, atualizados e de fácil compreensão;
> IV - pertinentes, completos, proporcionais e não excessivos em relação à finalidade que justificou sua coleta ou tratamento posterior;
> V - conservados de forma a permitir a identificação de seu titular por um período de tempo não superior ao necessário para as finalidades que justificaram sua coleta ou tratamento posterior; e
> VI - conservados por período não superior ao estabelecido em lei ou regulamento específico para cada setor.
> § 1º É vedado o tratamento de dados pessoais obtidos por meio de erro, dolo, coação e lesão.
> § 2º Os dados pessoais obtidos ou tratados de forma contrária à presente lei e à disciplina referente à proteção de dados não poderão ser utilizados e deverão ser cancelados.

O art. 14 repete os princípios norteadores dos tratamentos de dados pessoais elencados no artigo 8º. Não obstante, destaca-se inciso V que trata do tempo de armazenamento dos dados pessoais. O referido inciso não determinou o prazo. Patrícia Peck e equipe comentam, com relação ao inciso V, que, da mesma forma que foi indicado prazo geral de cinco anos para a renovação do consentimento para o tratamento dos dados no artigo 9º, inciso VI merece nova redação para se estabelecer um prazo máximo para guarda de dados caso inexistente o regulamento específico para cada setor.

Patrícia Peck e equipe ainda salienta que "*como a guarda dos dados pode ser necessária para investigação criminal ou para apuração de algum ato ilícito, entendemos ser aplicável o mesmo prazo de 5 anos e sob as mesmas condições que o artigo 9º, podendo ser estendido em casos excepcionais por Ordem Judicia*l."

> CAPÍTULO IV
> DOS DIREITOS DO TITULAR
> Art. 15. O titular dos dados poderá obter do responsável pelo tratamento a confirmação da existência de dados pessoais que lhe digam respeito, bem como o acesso aos dados em si, tanto diretamente, como por meio da ação de *habeas data*, nos termos da lei.
> § 1º As informações requeridas serão fornecidas, imediatamente, de forma simplificada ou, no prazo de 5 (cinco) dias, por meio de um extrato claro e completo, abrangendo a informação sobre a sua origem, bem como sobre a lógica, os critérios utilizados e a finalidade do respectivo tratamento.

> § 2º O fornecimento destas informações não importa em ônus para o titular dos dados.
> § 3º Estas informações, por escolha do titular, poderão ser fornecidas por escrito ou por meio eletrônico, seguro e idôneo para tal fim.
> § 4º A informação deve ser ampla e versar sobre a totalidade do registro existente, mesmo quando o requerimento compreender somente um aspecto dos dados pessoais do titular.
> § 5º Os dados pessoais serão armazenados de forma que permitam o exercício do direito de acesso.

O art. 15 se espelha no art. 43 do CDC, inclusive estabelece o mesmo prazo de cinco dias para informar ao titular dos dados pessoais se qualquer informação ao seu respeito se encontra na base de dados do responsável.

Ademais, o final do *caput* remete ao instituto do *habeas data* sendo este o adequado instrumento jurídico para acesso a banco de dados público.

O parágrafo primeiro do art. 15 ainda dispõe que é direito do titular o conhecimento da lógica/método aplicado para o tratamento dos seus dados. Contudo, Monteiro e Lima alertam que o método muitas vezes recebe proteção autoral e industrial. Ademais, o artigo não menciona obrigatoriedade do titular dos dados se fazer representado por terceiros, indicando que ele próprio poderá propor tais procedimentos.

> Art. 16. Mediante solicitação do titular dos dados, o responsável deverá, sem ônus, no prazo de 5 (cinco) dias:
> I - corrigir os dados pessoais que forem incompletos, inexatos ou desatualizados;
> II - cancelar, dissociar ou bloquear os dados pessoais que forem desnecessários, excessivos ou tratados em desconformidade com a presente lei.
> Parágrafo único. O responsável obriga-se, no prazo de 5 (cinco) dias, a comunicar aos destinatários das informações a realização de correção, cancelamento, dissociação e bloqueio dos dados.

O art. 16 trata da requisição para alteração de dados pessoais contidos em determinada base de dados. Monteiro e Lima entendem que a requisição não precisa ser motivada. Patrícia Peck e equipe salientam que o parágrafo único deste artigo merece complementação, pois não especifica qual meio de comunicação será utilizado para cumprir tal obrigação.

> Art. 17. O titular dos dados poderá opor-se, total ou parcialmente, ao tratamento de seus dados pessoais:

> I - sempre que tiver motivos legítimos, salvo nos casos em que o tratamento seja necessário para o cumprimento de uma obrigação imposta pela lei à pessoa responsável;
> II - quando seus dados forem utilizados para fins publicitários, ainda que tenham sido submetidos a um procedimento de dissociação.

O art. 17 dá ao titular dos dados a possibilidade de completo controle sobre fornecer ou não suas informações. Patrícia Peck e equipe afirmam pequeno conflito das normas, pois a oposição prevista pelo inciso II somente deveria ser aplicável caso não houvesse consentimento ou conhecimento prévio pelo titular, sob pena de dificuldade na aplicação do próprio tratamento de dados, pois sua finalidade mais recorrente seria para fins publicitários.

> Art. 18. Nos casos de descumprimento desta lei, o titular poderá pleitear os seus direitos perante a Autoridade de Garantia, na forma do regulamento.

O art. 18 cria nova instância administrativa. Monteiro e Lima elencam o rol de possibilidades à disposição do titular dos dados: (i) notificação ao responsável pelo tratamento; (ii) proposição de medida judicial; (iii) proposição de requisição administrativa à autoridade de garantia; e (iv) interposição de *habeas data*.

> Art. 19. O titular dos dados tem direito a não ser submetido a decisões que lhe afetem, de maneira significativa, unicamente com base em um tratamento automatizado de dados pessoais destinado a definir o perfil ou a personalidade do titular.
> § 1º Qualquer decisão desta natureza pode ser impugnada pelo titular, que tem o direito de obter informações do responsável pelo tratamento a respeito dos critérios desta avaliação e sobre o procedimento em que está se baseou.
> § 2º Admite-se esta modalidade de decisão nos casos em que tenha sido expressamente solicitada pelo titular e desde que garantidos o devido processo legal e a ampla defesa.

Patrícia Peck e equipe alertam que o *caput* do art. 19 faz menção de decisões às quais o titular pode ser submetido e que lhe afetem, sendo que, no entanto, não há delimitação de suas espécies e tampouco a origem, se administrativas, judiciais ou meramente decisões de mercado por sistemas informatizados.

> CAPÍTULO V
> TRATAMENTO DE DADOS SENSÍVEIS
> Art. 20. Nenhuma pessoa pode ser obrigada a fornecer dados sensíveis.

Conceito de dados sensíveis encontra-se no art. 4, inciso IV. Monteiro e Lima alertam que o conceito trazido de dados sensíveis não englobou os dados geográficos. Contudo, houve a inclusão como dados sensíveis dos dados de natureza genética.

> Art. 21. É proibida a formação de bancos de dados que contenham informações que, direta ou indiretamente, revelem dados sensíveis, salvo disposição legal expressa, respeitados os direitos de personalidade do titular, em especial a garantia de não discriminação.
> § 1º O tratamento de dados sensíveis será permitido quando:
> I - o titular tiver dado o seu consentimento livre, informado e por escrito, sempre que este tratamento for indispensável para o legítimo exercício das atribuições legais ou estatutárias de seus responsáveis.
> II - for realizado por associações e outras entidades sem fins lucrativos de natureza política, filosófica, religiosa ou sindical para a realização de finalidades lícitas e compreendendo os dados pessoais de seus inscritos, sempre que os dados não sejam comunicados ou difundidos para terceiros e quando o ente em questão determine medidas idôneas de garantia dos direitos do titular para o tratamento realizado;
> III - for necessário para a proteção da vida ou da incolumidade física do titular ou de um terceiro, nos casos em que o titular não possa prestar o próprio consentimento por impossibilidade física ou por incapacidade de compreensão;
> IV - for realizado unicamente com finalidades de pesquisa histórica, científica ou estatística;
> V - for relativo a dados manifestamente tornados públicos pelo seu titular;
> VI - for realizado por profissionais da área da saúde ou entidades sanitárias e se mostrar indispensável para a tutela da saúde do interessado; ou
> VII – for necessário para o exercício de funções próprias dos poderes de Estado, previstas em lei.
> § 2º Em qualquer hipótese, considerar-se-á ilegal o tratamento de dados sensíveis que for utilizado para fins discriminatórios.

O art. 21 proíbe a formação de dados sensíveis, salvo por expressa disposição legal ou consentimento livre do titular dos dados. Monteiro e Lima alertam que o conceito trazido de dados sensíveis não englobou os dados geográficos. Patrícia Peck e equipe por sua vez comentam que o inciso I do parágrafo primeiro merece reparo na redação, pois acabaria impedindo o tratamento regular de dados sensíveis pelas empresas que coletarem os dados de forma legítima, ficando em desvantagem inequívoca as organizações que trabalharem com internet.

Ademais, Patrícia Peck e equipe salientam que o inciso VII pode ser aprimorado, contemplando não apenas a lei, mas, também, para que este cumpra as funções institucionais às quais foi idealizado.

Por fim Patrícia Peck e equipe afirmam pequena incoerência, pois todo banco de dados sensíveis são discriminatórios, bastando lembrar que discriminar não significa prejuízo ou cometimento de crime, vez que significa diferenciar, separar ou distinguir e, portanto, nem sempre será negativo.

> Art. 22. A Autoridade de Garantia poderá indicar medidas de segurança e de proteção ao titular de dados sensíveis que deverão ser adotadas pelo responsável pelo tratamento.
>
> CAPÍTULO VI
> SEGURANÇA DOS DADOS
>
> Art. 23. O tratamento de dados pessoais será feito de modo a reduzir ao mínimo, mediante a adoção de medidas idôneas de segurança preventiva, o risco de sua destruição ou perda, de acesso não autorizado ou de tratamento não permitido pelo titular ou diverso da finalidade da sua coleta, independentemente do motivo.
> Parágrafo único. As medidas referidas no caput 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.

O art. 23 demonstra a preocupação com a questão da segurança da informação, tendo sido criado o "princípio da segurança física e lógica (Art. 8º, VII). Monteiro e Lima advertem que a diretriz a ser seguida é o que diz respeito aos bancos de dados, principais repositórios de informações que precisam ser desenhados de modo a impedir que, mesmo quando capturados por terceiros não autorizados, ainda assim, seja difícil o acesso aos dados ali contidos, privilegiando a utilização de criptografia.

> Art. 24. Um conjunto de medidas mínimas de segurança preventiva será publicado pela Autoridade de Garantia dentro de, no máximo, um ano após a entrada em vigor da presente lei, e atualizado periodicamente, com base na evolução da tecnologia e na experiência adquirida.

O art. 24 reafirma a necessidade de diária adaptação às alterações tecnológicas daqueles que lidam com os dados pessoais. Monteiro e Lima comentam importância em se observar as novidades trazidas em sede de normas da ANBT (Associação Brasileira de Normas Técnicas), ISO (Organização para Padronização), com especial atenção para as já publicadas normas ISO 27.001 e 27.002, previsões da *RSA Data Security*, RFC (*Request for Comments*) dentre outros.

> Art. 25. O subcontratado deve ter experiência, capacidade e idoneidade para garantir o respeito às disposições vigentes em matéria de tratamento de dados pessoais, e responderá solidariamente com o responsável pelos prejuízos causados pela sua atividade aos titulares dos dados.
> Parágrafo único. O subcontratado deverá realizar o tratamento segundo as instruções fornecidas por escrito pelo responsável, que, mediante inspeções periódicas, verificará a observância das próprias instruções e das normas sobre a matéria.

O art. 4º, inciso VIII traz o conceito de subcontratado que pode ser entendido como "administrador de banco de dados". Ademais, o art. 29 aborda a responsabilidade solidária entre cedente e cessionário.

> Art. 26 O responsável, o subcontratado ou qualquer outra pessoa que intervenha em qualquer fase do tratamento de dados pessoais obriga-se ao dever de segredo em relação aos mesmos, dever este que permanece após o término do respectivo tratamento ou do vínculo empregatício existente.

O art. 26 traz o dever de segredo, *ad eternum*, em relação aos dados tratados, por parte daqueles que tiveram contato com eles. Tal preocupação é pertinente tendo em vista que se pode ter contato com informações sensíveis que, caso liberadas sem qualquer preocupação, podem trazer inúmeros prejuízos às partes referidas.

> Art. 27. O responsável pelo tratamento deverá comunicar à Autoridade de Garantia e aos titulares dos dados, imediatamente, sobre o acesso indevido, perda ou difusão acidental, seja total ou parcial, de dados pessoais, sempre que este acesso, perda ou difusão acarretem riscos à privacidade dos seus titulares.
> Parágrafo único. Nos casos mencionados no caput, a Autoridade de Garantia poderá tomar as providências que julgar necessárias, no âmbito de suas competências, inclusive determinando ao responsável a ampla divulgação do fato em meios de comunicação.
>
> CAPÍTULO VII
> COMUNICAÇÃO E INTERCONEXÃO DOS DADOS PESSOAIS
> Art. 28. A comunicação ou a interconexão dos dados pessoais somente será permitida com o consentimento livre e expresso do titular e para o cumprimento de fins diretamente relacionados com as funções legítimas do cedente e do cessionário.
> § 1º O consentimento para a comunicação ou interconexão é revogável a qualquer tempo.
> § 2º O consentimento será dispensado quando:
> I - os dados forem provenientes de registros, atos ou documentos públicos acessíveis a qualquer pessoa, levando em consideração os limites estabelecidos para o acesso e publicidade destes dados;
> II - para o cumprimento de uma obrigação prevista em lei;

> III - quando for necessária para a proteção da vida ou da incolumidade física do titular ou de um terceiro, nos casos em que o titular não possa prestar o próprio consentimento por impossibilidade física ou por incapacidade de compreensão.

O art. 28, regra geral, sobre a comunicação e a interconexão dos dados pessoais, que somente serão permitidas com o consentimento livre e expresso do titular, para fins relacionados com as funções legítimas do cedente e do cessionário.

> Art. 29. O cessionário ficará sujeito às mesmas obrigações legais e regulamentares do cedente, inclusive quanto à responsabilidade solidária pelos danos eventualmente causados e ao dever de receber e processar impugnação e realizar correções.

O art. 29 traz a responsabilidade solidária entre o cedente e o cessionário.

> CAPÍTULO VIII
> DO TÉRMINO DO TRATAMENTO DOS DADOS PESSOAIS
>
> Art. 30. Os dados pessoais serão cancelados quando deixarem de ser necessários ou pertinentes para a finalidade que justificou sua coleta e tratamento.
> Parágrafo único. Lei ou regulamento poderá dispor sobre períodos máximos para o tratamento de dados pessoais em setores e situações específicas.

Monteiro e Lima ponderam que o caput do Art. 30 dá a impressão de que, após certo tempo, os próprios dados pessoais seriam cancelados. Contudo, o que se tem, é o cancelamento do tratamento deles. Diante disso afirmam os autores lacuna no que toca à exclusão dos dados pessoais, a partir do momento em que eles não fossem mais necessários ou a guarda deles não fosse pertinente.

> Art. 31. No término do tratamento dos dados pessoais, sem prejuízo dos direitos do titular, e sempre que houver necessidade ou pertinência, os dados podem ser:
> I - cedidos a terceiros, desde que destinados a tratamento para finalidades análogas àquelas para as quais foram colhidas e mediante o consentimento dos titulares;
> II - conservados para fins exclusivamente pessoais e não destinados à comunicação ou à difusão;
> III - conservados ou cedidos a terceiro, unicamente para finalidades históricas, estatísticas ou de pesquisa científica.

O inciso I do art. 31 trata da cessão dos dados pessoais a terceiros, mediante prévio consentimento do titular.

> CAPÍTULO IX
> TRATAMENTO DE DADOS PESSOAIS NO SETOR PÚBLICO
> Art. 32. A comunicação e interconexão de dados pessoais entre pessoas jurídicas de direito público será admitida nos casos em que suas competências não versem sobre matérias distintas, respeitados os direitos estabelecidos nesta lei.
> Parágrafo único. A comunicação de dados pessoais entre pessoas jurídicas de direito público com competências sobre matérias distintas será admitida:
> I - mediante expressa previsão legal, sempre no respeito aos direitos dos titulares dos dados; ou
> II - quando for necessária para a realização das suas competências institucionais.

O art. 32 trata da comunicação e da interconexão de dados pessoais entre pessoas jurídicas de direito público. Importante salientar o art. 5º, X que protege e garante os direitos de privacidade e de intimidade. Monteiro e Lima destacam que não se exige autorização do titular dos dados para tal cessão, o que poderia dar maior liberdade para troca dessas informações entre os distintos órgãos governamentais, mas, em contrapartida, ampliaria as chances de vazamento desses dados.

Patrícia Peck e equipe salientam que para melhores condições de aparelhamento de informações e dados, as pessoas jurídicas de direito público devem possuir total liberdade para realizar comunicação ou interconexão de dados entre seus entes, evitando a duplicidade ou não correspondência de informações e dados sobre um mesmo indivíduo. Este procedimento, segundo Patrícia Peck e equipe, valoriza todas as áreas de aplicação do Direito e homenageia a soberania do Estado sobre os dados que estão sob seu manto, não ficariam em desvantagem se comparado com a iniciativa privada que há tempos constrói bases de dados com informações dos indivíduos e utiliza sistema de cruzamento e comparação entre eles para chegar a determinado objetivo.

> Art. 33. Os responsáveis pelos bancos de dados públicos poderão, mediante decisão fundamentada e somente pelo período necessário, negar o cancelamento e a oposição ao tratamento dos dados pessoais, quando for indispensável para:
> I - a proteção da ordem pública;
> II - a proteção de direitos de terceiros;
> III – não obstaculizar a atuação judicial ou administrativa em curso, vinculadas à investigação sobre o cumprimento de obrigações tributárias, o desenvolvimento de funções de controle da saúde e do meio ambiente e a verificação de infrações administrativas.

> CAPÍTULO X

TRATAMENTO DE DADOS PESSOAIS NO SETOR PRIVADO

Art. 34. Toda entidade privada que realize o tratamento de dados pessoais para o desenvolvimento de suas atividades e conte com mais de duzentos empregados deverá apontar um diretor responsável pelo tratamento de dados pessoais.

§ 1º O diretor responsável pelo tratamento de dados pessoais deverá zelar, de forma independente, pela observância das disposições da presente lei.

§ 2º As atividades do diretor responsável pelo tratamento de dados pessoais consistem, entre outras, em:

I – atuar como o correspondente imediato da Autoridade de Garantia;

II - orientar os demais funcionários a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

III - manter uma relação dos tratamentos de dados pessoais realizados pela empresa, imediatamente acessível pelos titulares que requisitem seus próprios dados pessoais.

§ 3º A entidade informará à Autoridade de Garantia sobre a identidade do diretor responsável pelo tratamento de dados pessoais.

CAPÍTULO XI

TRANSFERÊNCIA INTERNACIONAL DE DADOS

Art. 35. A transferência internacional de dados pessoais somente é permitida para países que proporcionem um nível de proteção de dados equiparável ao da presente lei, salvo as seguintes exceções:

I - quando o titular tiver manifestado o próprio consentimento livre, expresso e informado para a transferência;

II - quando for necessária para a execução de obrigações derivadas de um contrato do qual o titular for parte;

III - quando for necessária para a garantia de um interesse público relevante previsto em lei;

IV – quando for necessária para a cooperação internacional entre órgãos públicos de inteligência e de investigação, de acordo com os instrumentos de direito internacional a que o Brasil se vincule;

V - quando for necessária para a defesa de um direito em juízo, se os dados forem transferidos exclusivamente para esta finalidade e pelo período de tempo necessário;

VI - quando for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro, se o titular não puder fornecer o próprio consentimento por impossibilidade física, por incapacidade de agir ou de compreender.

Art. 36. A Autoridade de Garantia reconhecerá o caráter adequado do nível de proteção de dados do país de destino levando em conta a legislação em vigor neste país e as demais circunstâncias relativas à transferência de dados.

Parágrafo único. Para os fins do previsto no caput, a Autoridade considerará a natureza dos dados, as normas gerais e setoriais presentes em seu ordenamento, a observância dos princípios de proteção de dados e das medidas de segurança previstas.

Art. 37. A Autoridade de Garantia poderá autorizar uma transferência ou série de transferências para um país estrangeiro que não disponha de um nível adequado de proteção quando o responsável pelo tratamento ofereça garantias suficientes em relação à proteção da privacidade dos titulares,

às medidas de segurança adotadas e a possibilidade do exercício dos direitos dispostos nesta lei.
Parágrafo único. A transferência de dados pessoais ao exterior, neste caso, somente poderá ocorrer após a autorização expressa da Autoridade de Garantia.

TÍTULO II
TUTELA ADMINISTRATIVA
CAPÍTULO I
AUTORIDADE DE GARANTIA

Art. 38. É criado o Conselho Nacional de Proteção de Dados Pessoais, com autonomia administrativa, orçamentária e financeira, com a atribuição de atuar como Autoridade de Garantia quanto à proteção de dados pessoais, cuja estrutura e atribuições serão estabelecidas em legislação específica.

Art. 39. Compete ao Conselho Nacional de Proteção de Dados Pessoais:
I - zelar pela observância desta lei, de seu regulamento e do seu regimento interno;
II - planejar, elaborar, propor, coordenar e executar ações da política nacional de proteção de dados pessoais;
III - editar normas e provimentos sobre matérias de sua competência;
IV - aprovar seu regimento interno;
V - receber, analisar, avaliar e encaminhar consultas, denúncias, reclamações ou sugestões apresentadas por titulares de dados pessoais, entidades representativas ou pessoas jurídicas de direito público ou privado, referentes à proteção de dados pessoais, nos termos do regulamento;
VI – aplicar, de ofício ou a pedido de parte, conforme o caso, sanções, medidas corretivas e medidas preventivas que considere necessárias, na forma desta lei;
VII – criar, manter e publicar, para fins de transparência, um registro de bancos de dados pessoais de caráter de categorias e setores que considere relevantes, nos termos de regulamento;
VIII - verificar se os tratamentos respeitam as normas legais e os princípios gerais de proteção de dados;
IX - promover o conhecimento entre a população das normas que tratam da matéria e de suas finalidades, bem como das medidas de segurança de dados;
X - vetar, total ou parcialmente, o tratamento de dados ou prover seu bloqueio se o tratamento se torna ilícito ou inadequado, nos termos de regulamento;
XI - reconhecer o caráter adequado do nível de proteção de dados do país de destino no caso de transferência internacional de dados pessoais, bem como autorizar uma transferência ou série de transferências para países terceiros que não contem com este nível adequado;
XII – determinar ao responsável pelo tratamento de dados pessoais, quando necessário, a realização de estudo de impacto à privacidade, na forma de regulamento.
XIII - desenvolver outras atividades compatíveis com suas finalidades.

> Art. 40. Os Estados, o Distrito Federal e os Municípios poderão criar suas próprias autoridades de proteção de dados pessoais, com competência concorrente e nas suas respectivas áreas de atuação administrativa.

O art. 40 autoriza a criação de diversas autoridades de proteção de dados pessoais, por parte dos Estados, Distrito Federal e dos Municípios.

> CAPÍTULO II
> SANÇÕES ADMINISTRATIVAS
> Art. 41. Sem prejuízo das sanções civis e penais cabíveis e de outras sanções administrativas a serem definidas em normas específicas, as infrações das normas previstas nesta Lei ficam sujeitas, conforme o caso, às seguintes sanções administrativas:
> I - multa;
> II – bloqueio dos dados pessoais;
> III – dissociação dos dados pessoais;
> IV – cancelamento dos dados pessoais;
> V – proibição do tratamento de dados sensíveis;
> VI – suspensão temporária de atividade; e
> VII – proibição de funcionamento do banco de dados.
> § 1º As sanções previstas neste artigo serão aplicadas pela Autoridade de Garantia, no âmbito de sua atribuição, podendo ser aplicadas cumulativamente, inclusive por medida cautelar, antecedente ou incidente de procedimento administrativo.
> § 2º As condições e procedimentos para a aplicação das sanções previstas, que devem ser graduadas em razão da gravidade, extensão da violação, natureza dos direitos pessoais afetados, reincidência e dos prejuízos dela derivados, serão determinados por meio de regulamentação.

O art. 41 traz o rol de consequências administrativas e cíveis do descumprimento das normas trazidas. Contudo, importante salientar que não há a previsão de aplicação de penas em âmbito criminal.

> Art. 42. A multa será estipulada:
> I - no caso de empresa, em até vinte por cento do valor do faturamento bruto no seu último exercício, excluídos os impostos;
> II - No caso das demais pessoas físicas ou jurídicas de direito público ou privado, bem como quaisquer associações de entidades ou pessoas constituídas de fato ou de direito, ainda que temporariamente, com ou sem personalidade jurídica, não sendo possível utilizar-se o critério do valor do faturamento bruto, em montante não inferior a R$ 2.000,00 (dois mil reais) e não superior a R$ 6.000.000,00 (seis milhões de reais).
> Parágrafo único. Em caso de reincidência, as multas cominadas serão aplicadas em dobro, não se aplicando, em tal hipótese, o limite máximo indicado no inciso II.

> Art. 43. Sem prejuízo das sanções cabíveis, a Autoridade de Garantia, atuando de ofício ou a pedido de parte, deverá impor, aos responsáveis

que incorram em infração às normas desta lei, as medidas corretivas que considere necessárias para reverter os efeitos danosos que a conduta infratora tenha causado ou para evitar que esta se produza novamente no futuro, fixando o valor da multa diária pelo seu descumprimento.
§ 1º As decisões administrativas transitadas em julgado que apliquem medidas corretivas em favor do titular dos dados constituem título executivo extrajudicial.
§ 2º Sempre que as medidas corretivas se dirigirem a um titular específico, é deste a legitimidade para executar a decisão.

Art. 44. Em qualquer fase do processo administrativo é facultado à Autoridade de Garantia adotar medidas preventivas, de ofício ou a pedido de parte, quando houver indício ou fundado receio de que o representado, direta ou indiretamente, cause ou possa causar à coletividade lesão irreparável ou de difícil reparação no âmbito da proteção de dados pessoais, ou torne ineficaz o resultado final do processo, fixando o valor da multa diária pelo seu descumprimento.

TÍTULO III
CÓDIGOS DE BOAS PRÁTICAS
Art. 45. Os responsáveis pelo tratamento de dados pessoais, individualmente ou através de organizações de classe, poderão formular códigos de boas práticas que estabeleçam as condições de organização, regime de funcionamento, procedimentos aplicáveis, normas de segurança, padrões técnicos, obrigações específicas para os diversos envolvidos no tratamento e no uso de dados pessoais e demais quesitos e garantias para as pessoas, com pleno respeito aos princípios e disposições da presente lei e demais normas referentes à proteção de dados.
§ 1º Os códigos de boas práticas vincularão os respectivos responsáveis pelo tratamento de dados e os membros de uma determinada classe profissional.
§ 2º A Autoridade de Garantia solicitará às respectivas organizações de classe a elaboração dos códigos de boas práticas quando julgar conveniente e poderá participar de sua elaboração.
§ 3º Entre outras categorias profissionais, a Autoridade de Garantia priorizará o fomento à elaboração de códigos de boas práticas em tema de:
I - vigilância e monitoramento;
II - publicidade e marketing direto;
III - bancos de dados de proteção ao crédito;
IV - seguros; e
V - demais matérias pertinentes.
§ 4º Os códigos de boas práticas serão depositados na Autoridade de Garantia, que poderá não aprová-los se estiverem em desconformidade com as disposições legais e regulamentares sobre a matéria, ao que seguirá uma solicitação para que sejam feitas as modificações necessárias e indicadas.
§ 5º Os códigos de boas práticas serão disponibilizados publicamente e deverão ser atualizados sempre que se demonstrar necessário.

TÍTULO IV
DISPOSIÇÕES FINAIS E TRANSITÓRIAS

> Art. 46. Os direitos previstos nesta lei não excluem outros, decorrentes de tratados ou convenções internacionais de que o Brasil seja signatário, da legislação interna ordinária, bem como de regulamentos expedidos pelas autoridades administrativas competentes.
>
> Art. 47. Ficam revogados os artigos de 2º, 3° e 4º da Lei 9.507, de 12 de novembro de 1997.
>
> Art. 48. Esta Lei entrará em vigor no prazo de 90 dias contados da data da sua publicação.

A estrutura do anteprojeto parece similar à utilizada pelo Uruguai e Argentina. Patrícia Peck e equipe acreditam que o referido anteprojeto, possui maior autonomia e capacidade de agir independentemente de ordens do Poder Judiciário, facilitando o funcionamento da instituição e aumentando o grau de eficácia do texto legal.

Por fim salienta-se que recentemente Brasil, Alemanha e China iniciaram cooperação para proteção de dados pessoais. O encontro foi promovido pelo *Privacy International* - Ministério Federal da Justiça e da Defesa do Consumidor alemão, em Berlim, dando início a uma troca política e técnica entre Brasil, China e Alemanha sobre o tema. O objetivo da cooperação é a confecção de uma pesquisa comparativa sobre a situação atual da proteção de dados do consumidor que produzirá recomendações para o estreitamento da cooperação no futuro[19].

[19] Artigo disponível em: http://oglobo.globo.com/economia/defesa-do-consumidor/brasil-alemanha-china-iniciam-cooperacao-para-protecao-de-dados-pessoais-14528535#ixzz3L4WVpe80. Acesso em 05/12/2014.

5. DIREITO COMPARADO.

O tratamento autônomo da proteção de dados pessoais é uma tendência hoje fortemente enraizada em diversos ordenamentos jurídicos, que veio a formar as bases para o que vem sendo tratado, hoje, como um direito fundamental à proteção de dados.

5.1 Sistema Europeu de Proteção de Dados Pessoais[20] [21]

- Começou a ser desenvolvido, na Europa, a partir do final da década de 1960. Podem ser descritos como seus antecedentes históricos tanto o artigo 12 da Declaração Universal dos Direitos do Homem, como o artigo 8º do Convênio para Proteção de Direitos Humanos e Liberdades Fundamentais, pactuado em Roma, no ano de 1950. Figuram também nesta lista de influências os artigos 17 e 18 do Pacto de Direitos Civis e Políticos, firmado em Nova Iorque no ano de 1966.

- Em 23 de janeiro de 1970, a Resolução nº 428 da Assembleia Parlamentar do Conselho da Europa, também conhecida como "Declaração sobre os meios de comunicação em massa e os Direitos Humanos" (*Declaration on mass communication media and Human Rights*), trouxe novamente a discussão sobre a necessidade de proteger a vida privada em face dos novos meios informáticos.

- Em 1981, foi aprovado, pelo Conselho da Europa a Convenção n.º 108, que firmou as bases principiológicas sobre a proteção dos indivíduos quanto ao tratamento de dados pessoais. Este foi o primeiro texto jurídico unificado sobre a matéria, que se propôs a garantir, no território de cada país-membro, o respeito aos direitos e liberdades fundamentais de todas as pessoas, independentemente de suas nacionalidades ou residências, atendendo, também, à proteção do tratamento automatizado de dados pessoais.

- Em 1995, o Parlamento Europeu e o Conselho da Europa aprovaram a Diretiva Comunitária n.º 95/46/1995, também conhecida como "Diretiva de Proteção de Dados" ou simplesmente "DPD", que regulamenta o tratamento e a livre circulação dos dados

[20] RUARO, Regina Linden; RODRIGUEZ, Daniel Piñero. *O direito à proteção dos dados pessoais: uma leitura do sistema europeu e a necessária tutela dos dados sensíveis como paradigma para um sistema jurídico brasileiro*. Disponível em: http://www.dfj.inf.br/Arquivos/PDF_Livre/11_Dout_Nacional_1.pdf. Acesso em 02/12/2014.

[21] VASQUEZ, Rafael Ferraz. *A proteção de dados pessoais nos Estados Unidos, União Europeia e América do Sul: Interoperabilidade com a proposta de marco normativo no Brasil*. Disponível em: < http://www.publicadireito.com.br/artigos/?cod=87682805257e619d>. Acesso em 21/11/2014.

pessoais, a qual marcou o direito comunitário europeu, na medida em que estabeleceu o dever dos Estados de criarem códigos de condutas nacionais e comunitários, para que fosse possível dar maior efetividade às disposições da Diretiva.

- Acentuou que a proteção dos dados pessoais deveria ser aplicada tanto ao tratamento automatizado de dados como ao tratamento manual, da mesma forma que a observância de suas determinações deveria se dar tanto pelo setor público quanto pelo setor privado.

- Uma grande motivação para se inspirar na "DPD" é a regra geral de proibição de exportação de dados pessoais da União Europeia a países fora do Espaço Econômico Europeu, caso o país destinatário dos dados não ofereça um nível de proteção de dados equivalente àquele Europeu. Consequentemente, de forma a qualificar como país apto a receber dados privados inúmeros países optaram por reproduzir em suas legislações àquelas existentes na DPD, facilitando assim a sua aprovação pela Comissão Europeia e consequente recebimento de dados pessoais sem a necessidade de requerer autorizações a cada transferência, a exemplo da Argentina e do Uruguai.

- Posteriormente, a Diretiva 97/66CE, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das telecomunicações, complementa a diretiva anterior, trazendo, por exemplo, determinações de segurança em determinados setores. Assim, havendo risco especial de violação da segurança de rede dos serviços de telecomunicações acessíveis ao público, o seu fornecedor estará obrigado a informar tal fato aos assinantes e quais as possíveis soluções, incluindo os respectivos custos da reparação pretendida.

- Em 2002 foi promulgada Diretiva 2002/58/CE buscando regulamentar a proteção de dados pessoais no âmbito da comunicação eletrônica. Não trouxe inovações ao ordenamento da comunidade europeia, mas buscou trazer a realidade tecnológica.

- Em 2006 veio a Diretiva 2006/24/CE que dispõe sobre a conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrônicas publicamente disponíveis ou de redes públicas de comunicações, salienta a necessidade da tutela do direito à privacidade e à intimidade por parte dos Estados-membros.

Oportuno destacar que sendo a Diretiva 95/46[22] reproduzida de maneira recorrente em legislações estrangeiras, importante se faz analisar algumas previsões. Um dos conceitos mais importantes trazidos na DPD é o de dados pessoais, definido pelo seu artigo 2º como[23]:

> (...) qualquer informação relativa a uma pessoa singular identificada ou identificável («pessoa em causa»); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social.(VASQUEZ, 2014)

Ademais, A DPD é aplicável a cidadãos estrangeiros, sendo, portanto, bastante amplo. A independência da nacionalidade é resultado da vontade legislativa de buscar sempre a aplicação da DPD aos dados pessoais, buscando proteger uma maior quantidade de dados pessoais.

Um último aspecto, fundamental para entender a estrutura europeia de proteção de dados, é o esquema de fiscalização e punição pelo descumprimento das regras de proteção de dados. Cada estado membro europeu, possui uma autoridade de controle com total independência nas suas funções, a qual terá competência para investigar, intervir e punir. As sanções pelo descumprimento foram deixadas para serem definidas a nível nacional de cada país da União Europeia[24].

Assim, conclui-se que a legislação europeia é o grande exemplo quando o assunto é proteção de dados pessoais. A Diretiva 95/46 (“Diretiva de Proteção de Dados” ou simplesmente “DPD”) estabeleceu verdadeira referência na expansão de leis sobre proteção de dados. Ademais, tem-se que inúmeros outros países, dentre eles muitos da

---

[22] Em primeiro lugar, cabe ressaltar que, por se tratar de uma diretiva (e não um regulamento europeu), a mesma necessitou implementação interna nos diversos países membro da União Europeia. Portanto, a mesma não é diretamente aplicável a nível nacional, embora sirva de base para as leis nacionais.

[23] VASQUEZ, Rafael Ferraz. *A proteção de dados pessoais nos Estados Unidos, União Europeia e América do Sul: Interoperabilidade com a proposta de marco normativo no Brasil*. Disponível em: < http://www.publicadireito.com.br/artigos/?cod=87682805257e619d>. Acesso em 21/11/2014.

[24] VASQUEZ, Rafael Ferraz. *A proteção de dados pessoais nos Estados Unidos, União Europeia e América do Sul: Interoperabilidade com a proposta de marco normativo no Brasil*. Disponível em: < http://www.publicadireito.com.br/artigos/?cod=87682805257e619d>. Acesso em 21/11/2014. *Ibidem*

América do Sul, optaram por seguir o seu exemplo e legislarem sobre o assunto de maneira quase idêntica à europeia.[25]

5.2 Sistema Argentino de Proteção de Dados Pessoais

- Foi o primeiro país da América Latina a receber a aprovação europeia para receber dados pessoais (outorga ocorrida em 2002).

- A proteção de dados pessoais deriva da sua Constituição e é regulamentada pela Lei n.º 25.326 sobre proteção de dados pessoais (LPDP) e do Decreto Regulamentar n.º 1558/2001 (Decreto).

- A LPDP foi inspirada na legislação europeia, contudo possui diferenças relevantes, como por exemplo: (i) define dados pessoais como sendo informações que identifica ou tornam identificável uma pessoa física ou jurídica (há inserção da proteção de pessoas jurídicas no escopo de proteção de dados pessoais, o que não ocorre na legislação europeia) e (ii) com relação à abrangência da norma, a lei argentina prevê a aplicação de suas leis quando os dados versarem sobre residentes em solo argentino, sejam eles nacionais ou não, enquanto que o modelo europeu prevê a aplicação das leis em caso da empresa responsável pelo tratamento se localizar naquele território ou quando houver o uso do equipamento em solo europeu.

- Sua Constituição prevê o instituto do *habeas data* (artigo 43.3), bem como eleva à categoria de direito fundamental o direito à proteção de dados. Por sua vez, a LPDP estabelece direitos e deveres, cria os órgãos de supervisão de proteção de dados e estabelece sanções em caso de descumprimento.

- Há a proibição de exportação de dados para países que não possuam um nível de proteção equivalente ao argentino (igual ao modelo europeu).

- A atual lei argentina é uma versão menos rígida de um projeto de lei apresentado e altamente criticado durante a sua proposição. O Projeto de Lei 24.745 acabou sendo rejeitado pelo executivo daquele país em razão do padrão considerado alto para a obtenção do consentimento para processamento de dados e o seu compartilhamento. Embora com um nível de proteção menor que o

[25] VASQUEZ, Rafael Ferraz. *A proteção de dados pessoais nos Estados Unidos, União Europeia e América do Sul: Interoperabilidade com a proposta de marco normativo no Brasil*. Disponível em: < http://www.publicadireito.com.br/artigos/?cod=87682805257e619d>. Acesso em 21/11/2014.

originalmente proposto, a atual legislação argentina, embora com a ressalva de que haveria necessidade de aguardar a interpretação e efeitos ao longo dos anos, foi aprovada pela Comissão Europeia como fornecendo um nível de proteção equiparado ao Europeu (UNIÃO EUROPEIA, 2002) e, portanto, dados pessoais oriundos da União Europeia já poderiam ser transferidos para aquele país sem maiores restrições.

5.3 Sistema Uruguaio de Proteção de Dados Pessoais

- Segue modelo pioneiro argentino na América Latina, passando pelo "crivo" da Comissão Europeia, sendo classificado a partir de 2010 como país com normas de proteção de dados adequada para receber dados da União Europeia.

- Em consequência do exposto acima, tem-se que a sua legislação é bastante semelhante àquela europeia e, consequentemente, à Argentina.

- Constituição Uruguaia não prevê o direito à proteção de dados, mas possibilita a inclusão de outros direitos fundamentais por meio de legislação inferior, na forma dos artigos 72 e 332. Tal previsão, como direito fundamental, é trazida pelo artigo primeiro da Lei 18.331 sobre proteção de dados e a ação de *habeas data*. Tal lei é regulamentada pelo Decreto 414/2009, que em seu preâmbulo, expressamente faz referência à Diretiva 95/46/EU (DPD), afirmando ser conveniente ajustar-se a tal legislação de direito comparado a qual é mais aceita do ponto de vista internacional. Embora não encontremos de maneira expressa tal afirmativa em outras legislações, parece ser exatamente este o espírito dos legisladores ao criarem normas de proteção de dados, seja na América Latina ou não.

- A definição de dados pessoais é parecida com a legislação da argentina, visto que incluem dados das pessoas jurídicas. Há também a classificação de dados sensíveis.

- Outra semelhança encontrada é a vedação de exportação de dados a países sem um nível equiparado de proteção de dados. Ao contrário da Argentina, a legislação uruguaia prevê a utilização de cláusulas contratuais para a obtenção de autorização.

- Criação de uma autoridade de proteção de dados, os princípios norteadores, e a implementação de um sistema de fiscalização e punição administrativa nos casos de descumprimento.

Como era de se esperar, a legislação uruguaia possui diversas semelhanças com a DPD, no entanto é quase um espelho da legislação argentina sobre a matéria. Como esperado, o legislador uruguaio inovou em questões pontuais e manteve a estrutura encontrada na DPD.

5.4 Sistema Chileno de Proteção de Dados Pessoais

- Constituição chilena prevê em seu Artigo 19(4) o direito à vida privada. Em 1999, o Chile aprovou a Lei 19.628 referente à "Proteção da Vida Privada" e no ano seguinte o Decreto 779/2000 que a regulamenta. Apesar de ser posterior à DPD, não houve por parte do Chile nenhuma inspiração na legislação europeia, sendo ainda nos dias de hoje considerada como "inadequada" desde o ponto de vista Europeu.

- Tal inadequação, em outras palavras, significa que dados privados demorarão até 7 meses para serem transferidos para o Chile, enquanto que para a Argentina, país considerado adequado pela Comissão Europeia, a mesma transferência demorará um dia.

- Principais críticas: omissão com relação a itens essenciais para uma lei de proteção de dados, tais como: princípio da finalidade, ausência de sanções e previsão sobre uma autoridade de controle de proteção de dados.

- Há projeto de lei tramitando no congresso desde 2008. Espera-se que o Chile venha a se tornar mais um país a legislar de maneira semelhante à europeia em matéria de proteção de dados pessoais, alterando a sua legislação atual.

5.5 Sistema Peruano de Proteção de Dados Pessoais[26]

- Legislação sobre proteção de dados foi aprovada em 2011 (Lei 29.733).

[26] VASQUEZ, Rafael Ferraz. *A proteção de dados pessoais nos Estados Unidos, União Europeia e América do Sul: Interoperabilidade com a proposta de marco normativo no Brasil*. Disponível em: < http://www.publicadireito.com.br/artigos/?cod=87682805257e619d>. Acesso em 21/11/2014.

- A Lei 29.733/11 ainda carece de regulamentação, mas é noticiado que a implementação desse novo marco jurídico será fruto de uma cooperação direta com a agência de proteção de dados espanhola, AEPD.

- Não se nota grande diferença entre as definições da lei peruana e aquelas da Diretiva 95/46.

5.6 Sistema Mexicano de Proteção de Dados Pessoais[27]

- Em 2010, o governo mexicano aprovou a Lei de Proteção de Dados Pessoais e o seu correspondente regulamento em dezembro de 2011. A implementação de um esquema de proteção de dados privados passou, inclusive, por uma reforma constitucional, a qual incluiu a proteção de dados privados como um direito expressamente reconhecido por lei bem como atribuindo competência ao congresso para legislar sobre o assunto.

- Uma inovação criada pela legislação mexicana é a divisão dos dados pessoais em três categorias diferentes: patrimoniais, financeiros e sensíveis.

- Lei mexicana também foi inspirada na Diretiva 95/46 da União Europeia.

5.7 Sistema Americano de Proteção de Dados Pessoais[28]

- Distinto do sistema europeu.

- Precedente oriundo do caso Katz vs. *United States* em 1967, decidido pela Suprema Corte. Fundamento da privacidade encontra-se na quarta emenda da Constituição Americana.

- Prevalece esquema de proteção de dados segmentado por setores, tipo de dados e até estado, estando, portanto, fragmentada. Tal característica acarretou que o regime americano não foi tudo como modelo para nenhum outro país.

[27] *Ibdem*.
[28] *Ibdem*.

5.8 Sistema do Reino Unido de Proteção de Dados Pessoais

- No âmbito do Reino Unido, existe o Ato de Proteção de Dados de 1998, do Parlamento (*Data Protection Act* 1998), de 16/07/1998.

- Principais princípios para o processamento de dados pessoais: (i) o processamento deve justo e legal; (ii) os dados pessoais devem ser obtidos para um ou mais propósitos especificados e legais e não devem ser processados de maneira incompatível com esses propósitos; (iii) os dados pessoais devem ser adequados, relevantes e não excessivos em relação aos propósitos para os quais eles são processados; (iv) devem ser precisos e mantidos atualizados; (v) não devem ser guardados por tempo maior que o necessário; (vi) devem ser processados de acordo os direitos pessoais dos indivíduos; (vii) devem ser adotadas medidas técnicas e organizacionais para impedir acesso não autorizado, processamento ilegal, perda acidental, destruição ou danos aos dados; e (viii) os dados pessoais não devem ser transferidos para fora da Área Econômica Europeia, a não ser sob garantia de adequado nível de proteção aos direitos e liberdades dos indivíduos detentores.

- Entidade Supervisora de dados é o *Data Protection Commissioner* e há a definição de um Tribunal de Proteção de Dados.

- A Entidade Supervisora tem poder para, dentre outras atividades, requerer a adequação legal do controlador de dados, receber denúncias, realizar diligências e determinações aos controladores de dados.

- São garantidos às pessoas o direito de acesso a seus dados pessoais; o direito de prevenir o processamento que possa causar estresse ou relativo a *marketing* direto; alguns direitos relativos a processos de decisão automática; o direito de compensação em caso de violação de certos requerimentos da legislação; e o direito de retificar, bloquear, apagar e destruir dados pessoais imprecisos.

- Há a definição de dados pessoais sensíveis.

- O processamento de dados pessoais somente é permitido se houver registro do controlador de dados na Entidade Supervisora.

- Há a criação de certos tipos penais por ofensa à legislação de proteção de dados pessoais.

- São estabelecidas exceções à aplicação da legislação quando se trata de segurança nacional, prevenção e detecção de crime, apreensão e processo de criminosos, saúde física ou mental, jornalismo, literatura e arte, pesquisa, história e estatística, dados relacionados a procedimentos legais, propósitos domésticos, dentre outras situações.

6. CONCLUSÃO

Por meio de um trabalho coordenado e interdependente entre as equipes da SE e da Universidade de Brasília, as atividades de elaboração deste RT foram planejadas, discutidas, executadas e documentadas.

Atualmente o Brasil dispõe de uma proteção dispersa e não específica sobre o tema proteção de dados. Menções aparecem em capítulos, artigos, parágrafos e incisos de diferentes normas legislativas e em decisões jurisprudenciais. Nota-se que a proteção de dados pessoais é raramente tratada como um direito fundamental no ordenamento pátrio. A tecnologia deve permitir ao indivíduo efetivar as conquistas da civilização, sem ferir o direito à inviolabilidade da vida privada.

Ao se analisar o Anteprojeto Brasileiro de Proteção de Dados Pessoais verifica-se a necessidade de esclarecimentos e aprofundamentos em determinados artigos e incisos especialmente nos que tratam da titularidade dos dados, da segurança dos repositórios de dados públicos e privados, da necessidade de criação de entidade regulatória autônoma, e da ausência, no momento, de aplicação de penas em âmbito criminal.

No contexto mundial, houve a formação de dois modelos principais: o modelo da União Europeia, rígida e institucional, que interpreta os dados pessoais como direito; e o modelo dos Estados Unidos, liberal e mercantil, que entende dados pessoais como propriedade e encontra-se em normas esparsas.

Nos demais países, onde tais legislações ainda se encontram em debate, vive-se grande pressão diplomática e comercial para a adoção de algum dos dois modelos.

A proliferação de novas tecnologias e, principalmente, da Internet no país pressiona para a existência de marcos legais. Considerando-se que o objetivo do texto do Anteprojeto não é somente a proteção dos dados pessoais, mas também o estabelecimento de um paradigma jurídico - que possa servir de sustentáculo para investimentos econômicos e desenvolvimento tecnológico - o dispositivo também poderia contemplar as proteções de ordem econômica e das relações de consumo que envolvem o cidadão.

As atividades envolvidas nesta etapa observaram formalmente a execução dos passos da metodologia elencada para gestão do projeto, PMI/PMBoK.

A equipe da UnB considera que teve acesso a todas as informações necessárias à boa condução dos trabalhos e que a disponibilização dessas informações pela equipe do MJ,

assim como as atividades conjuntas de análise e discussão, levou a etapa do projeto a bom termo.

BIBLIOGRAFIA

ABEMD. Proteção de Dados no Brasil – Linha do Tempo. Disponível em: <http://abemd.org.br/interno/cafe_030914_protecao_de_dados.pdf>. Acesso em 25/11/2014.

Brasil. A proteção de dados pessoais nas relações de consumo: para além da informação creditícia. Escola Nacional de Defesa do Consumidor – ENDC. coord. Danilo Doneda. Brasília: SDE/DPDC, 2010. Disponível em: http://www.vidaedinheiro.gov.br/docs/Caderno_ProtecaoDadosPessoais.pdf. Acesso em 01/11/2014.

CASTRO, Luiz Fernando Martins. *Proteção de dados pessoais – internacional e brasileiro*. Conferência proferida no "Congresso Internacional de Direito e Tecnologias da informação", realizado pelo Centro de Estudo Judiciários, nos dias 3 e 4 de 2002, no auditório do Superior Tribunal de Justiça. R. CEJ, Brasília. N.º 19, p. 40-45, out/dez. 2002.

DONEDA, Danilo. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. Disponível em: < http://www.estig.ipbeja.pt/~ac_direito/Consideracoes.pdf>. Acesso em 05/11/2014.

MONTEIRO, Renato Leite; LIMA, Caio César Carvalho. Comentários ao Anteprojeto de Lei sobre Proteção de Dados Pessoais. Disponível em: <http://securitybreaches.files.wordpress.com/2011/05/anteprojeto-de-lei-brasileiro-sobre-protecao-de-dados-pessoais.pdf>. Acesso em 11/11/2014.

MONTEIRO, Renato Leite; LIMA, Caio César Carvalho. Panorama brasileiro sobre a proteção de dados pessoais: discussão e análise comparada. Disponível em: http://www.atoz.ufpr.br/index.php/atoz/article/view/41/121. Acesso em 12/11/2014

PECK, Patrícia. Parecer: Contribuições para redação do anteprojeto de Lei. Proteção de Dados Pessoais. Disponível em http://culturadigital.br/dadospessoais/files/2011/05/Patricia-Peck-Pinheiro-Advogados-Prote%C3%A7%C3%A3o-de-Dados.pdf. Acesso em 11/11/2014.

PERLINGIERI, Pietro. *Perfis de Direito Civil.* Tradução de: Maria Cristina De Cicco. 2ª Ed. – Rio de Janeiro: Renovar, 2002.

VASQUEZ, Rafael Ferraz. A proteção de dados pessoais nos Estados Unidos, União Europeia e América do Sul: Interoperabilidade com a proposta de marco normativo no Brasil. Disponível em: < http://www.publicadireito.com.br/artigos/?cod=87682805257e619d>. Acesso em 21/11/2014.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Revista da Faculdade de Direito. São Paulo, v. 88, 1993.

TEPEDINO, Gustavo José Mendes. Cidadania e os direitos da personalidade . Revista Jurídica, Porto Alegre, 2004.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. O Direito à Proteção de dados frente a Medidas de Segurança e Intervenção Estatal. Revista NEJ – Eletrônica, vol.15, nº2, maio/ago, 2010

ONU. Assembleia Geral das Nações Unidas. DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS, 1948 – Disponível em http://unesdoc.unesco.org/images/0013/001394/139423por.pdf

BRASIL. A proteção de dados pessoais nas relações de consumo: para além da informação creditícia. Escola Nacional de Defesa do Consumidor – ENDC. Disponível em: http://www.vidaedinheiro.gov.br/docs/Caderno_ProtecaoDadosPessoais.pdf. Acesso em 01/11/2014

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil – disponível em www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 01/11/2014

BRASIL. A proteção de dados pessoais nas relações de consumo: para além da informação creditícia. Escola Nacional de Defesa do Consumidor – ENDC. Disponível em: http://www.vidaedinheiro.gov.br/docs/Caderno_ProtecaoDadosPessoais.pdf. Acesso em 01/11/2014

BRASIL. LEI No 10.406, DE 10 DE JANEIRO DE 2002. Institui o Código Civil – Disponível em http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm. Acesso em 01/11/2014

BRASIL. LEI Nº 8.078, DE 11 DE SETEMBRO DE 1990. Dispõe sobre a proteção do consumidor e dá outras providências – Disponível em http://www.planalto.gov.br/CCIVIL_03/leis/L8078.htm. Acesso em 01/11/2014

BRASIL. LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências. - Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em 01/11/2014

BRASIL. LEI Nº 7.232, DE 29 DE OUTUBRO DE 1984. Dispõe sobre a Política Nacional de Informática, e dá outras providências – Disponível em http://www.planalto.gov.br/ccivil_03/leis/L7232.htm. Acesso em 01/11/2014

BRASIL. PL 4060/2012 - Câmara dos Deputados. Dispõe sobre o tratamento de dados pessoais, e dá outras providências – Disponível em http://www2.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066. Acesso em 01/11/2014

BRASIL. PROJETO DE LEI DO SENADO 181 de 2014. Estabelece princípios, garantias, direitos e obrigações referentes à proteção de dados pessoais - Disponível em http://www.senado.gov.br/atividade/materia/detalhes.asp?p_cod_mate=117736. Acesso em 01/11/2014

BRASIL. PROJETO DE LEI DO SENADO 330 de 2013. Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências – Disponível em http://www.senado.gov.br/atividade/materia/detalhes.asp?p_cod_mate=113947. Acesso em 01/11/2014

BRASIL. PROJETO DE LEI DO SENADO 131 de 2013. Altera a Lei nº 9.249, de 26 de dezembro de 1995, para permitir a dedução, em dobro, do Imposto de Renda da Pessoa Jurídica, das despesas incorridas com a contratação de empregados com mais de cinquenta anos de idade – Disponível em http://www.senado.gov.br/atividade/materia/detalhes.asp?p_cod_mate=112362. Acesso em 01/11/2014

BRASIL. Lei n.º 12.965/2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil – Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 01/11/2014

Grossmann, Luís Osvaldo, Debate no Senado evidencia atraso em lei de proteção de dados pessoais. Convergência Digital, 02 DEZ 2014. Disponível em http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=38563&sid=4#.VIJM-jHF8ms. Acesso em 01/11/2014

O GLOBO. Brasil, Alemanha e China iniciam cooperação para proteção de dados pessoais. 11 NOV 2014. Disponível em: http://oglobo.globo.com/economia/defesa-do-consumidor/brasil-alemanha-china-iniciam-cooperacao-para-protecao-de-dados-pessoais-14528535#ixzz3L4WVpe80. Acesso em 05/12/2014

Universidade de Brasília – UnB

Centro de Apoio ao Desenvolvimento Tecnológico – CDT

Laboratório de Tecnologias da Tomada de Decisão – LATITUDE

www.unb.br – www.cdt.unb.br – www.latitude.eng.br