UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS I
CENTRO DE CIÊNCIAS JURÍDICAS
CURSO DE DIREITO

KAYSE CHAVES DA COSTA

PROTEÇÃO DE DADOS PESSOAIS:
Uma análise da legislação estrangeira e nacional

CAMPINA GRANDE
2016

KAYSE CHAVES DA COSTA

PROTEÇÃO DE DADOS PESSOAIS:
Uma análise da legislação estrangeira e nacional

Trabalho de Conclusão de Curso apresentado ao Curso de Bacharelado em Direito da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de Bacharela em Direito.

Área de concentração: Informática Jurídica.
Orientador(a): M.e. Marcelo D'Angelo Lara.

CAMPINA GRANDE
2016

C837p Costa, Kayse Chaves da.
Proteção de dados pessoais [manuscrito] : uma análise da legislação estrangeira e nacional / Kayse Chaves da Costa. - 2016.
42 p. : il. color.

Digitado.
Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Estadual da Paraíba, Centro de Ciências Jurídicas, 2016.
"Orientação: Prof. Me. Marcelo D'Angelo Lara, Departamento de Direito Público".

1. Proteção de Dados Pessoais. 2. Lei de Proteção de Dados. 3. Marco Civil da Internet. I. Título.

21. ed. CDD 342.02

KAYSE CHAVES DA COSTA

PROTEÇÃO DE DADOS PESSOAIS:
Uma análise da legislação estrangeira e nacional

Trabalho de Conclusão de Curso apresentado ao Curso de Bacharelado em Direito da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de Bacharela em Direito.

Área de concentração: Direito Cibernético.

Aprovada em: 23 / 05 / 2016.

BANCA EXAMINADORA

Prof. M.e. Marcelo D'Angelo Lara. (Orientador)
Universidade Estadual da Paraíba (UEPB)

Prof. M.e. Geovani Pereira Guimarães
Universidade Estadual da Paraíba (UEPB)

Prof. M.ª. Maria Cezilene Araujo de Morais
Universidade Estadual da Paraíba (UEPB)

The computer, with its insatiable appetite for information, its image of infallibility, its inability to forget anything that has been put into it, may become the heart of a surveillance system that will turn society into a transparent world in which our home, our finances, our associations, our mental and physical condition are laid bare to use most casual observer. (Miller, A).

SUMÁRIO

PROTEÇÃO DE DADOS PESSOAIS:
Uma análise da legislação estrangeira e nacional

Kayse Chaves da Costa[1]
Marcelo D'Angelo Lara[2]

RESUMO

O tratamento de dados pessoais por processos automatizados é uma atividade de risco. Considerando-se o movimento mundial relativo à segurança jurídica e aos marcos regulatórios para a proteção de dados pessoais, este artigo analisa os contornos jurídicos da proteção dos dados pessoais e explora suas principais definições no direito interno, fazendo uma breve análise e expondo o atual panorama no Brasil e analisando o Anteprojeto Brasileiro de Proteção de Dados Pessoais, com o escopo de esboçar a realidade do ordenamento pátrio, e no direito estrangeiro, em particular o dos Estados Unidos e o da União Europeia, traçando as origens do direito a proteção dos dados pessoais e de sua classificação como direito fundamental. Utilizando-se como método o levantamento de legislação, de doutrina e de jurisprudência nacional e internacional e obtendo-se como resultado a constatação de que atualmente o Brasil dispõe de uma proteção dispersa e não específica sobre o tema proteção de dados dispondo, apenas, de menções em capítulos, artigos, parágrafos e incisos de diferentes normas legislativas e em decisões jurisprudenciais. A proliferação de novas tecnologias e, principalmente, da *Internet* no país pressiona o Estado para a existência de marcos legais. O Anteprojeto de Proteção de Dados Pessoais objetiva não somente a proteção dos dados pessoais, mas também o estabelecimento de um paradigma jurídico que possa servir de sustentáculo para investimentos econômicos e para o desenvolvimento.

Palavras-Chave: Proteção de dados pessoais. Privacidade. Lei de Proteção de Dados.

1 INTRODUÇÃO

O surgimento, e posterior avanço, da Era Digital fomentou a necessidade de se repensar importantes aspectos relativos a institutos como os da organização social, da democracia, da tecnologia, da privacidade e da liberdade.

A revolução tecnológica já aconteceu, dispositivos eletrônicos móveis com uma conectividade à *Internet* cada vez mais rápida já fazem parte do dia a dia dos cidadãos em

[1] Graduanda em Direito na Universidade Estadual da Paraíba – UEPB. Email: kay.chaves@gmail.com.br
[2] Mestre em direito e professor substituto da Universidade Estadual da Paraíba – UEPB. E-mail: marcelodlara@hotmail.com

todo o planeta. E com esse avanço surgiram novos problemas, ou velhos problemas apenas em um ambiente novo.

A *Internet* passou uma ideia de que ninguém a regulamentava, ideia essa que parece prevalecer até hoje[3].

Desde que passou a viver em sociedade, o homem monitora seu progresso e coleta dados sobre si mesmo e sobre os indivíduos de sua convivência que interessem a diferentes finalidades.

Com as mudanças advindas da chamada sociedade da informação, a proteção da informação passou a ser extremamente frágil, pois praticamente qualquer informação pode ser pesquisada na Rede. A *Internet* constitui o maior exemplo de como as tecnologias de monitoramento e investigação têm evoluído. Aquele que acessa a *Internet* tem cada um de seus atos monitorados permanentemente. Há entidades denominadas provedores de conexão que identificam precisamente onde, quando e quão rápido o indivíduo acessou cada *site*, documentando que lojas visitou, por quais *links* se interessou, em qual ordem e por quanto tempo. Ademais, os dados coletados neste monitoramento cibernético são permanentes e, portanto, investigáveis por qualquer pessoa que tenha interesse em ter acesso a essas informações[4].

Diante disso, e, dada a amplitude da relevância do tema, este artigo se propõe a analisar o direito positivo dos ordenamentos jurídicos de outros países comparando-os com a legislação pátria, tendo em vista que o Brasil não possui legislação específica em relação a proteção de dados pessoais. Na busca dos resultados pretendidos, foram utilizados dois gêneros de pesquisa: teórico (com maior predominância) e empírico.

O trabalho aponta como conclusão que o Direito deve manifestar-se por meio da criação de normas que transcendam as evoluções tecnológicas. E não apenas isso, o seu enfoque deve não meramente ser direcionado a uma única nação, mas sim, ser global, motivo pelo qual o presente artigo mostra o desenvolvimento das diretrizes relacionadas à proteção dos dados pessoais no Brasil, União Europeia e nos Estados Unidos, constatando-se, à vista disso, a fragilidade protetiva do instituto na legislação brasileira.

---

[3] FINKELSTEIN. Maria Eugênia. *Direito do Comércio Eletrônico*. 2. ed. Rio de Janeiro: Elsevier: 2011, p11.
[4] FINKELSTEIN. Maria Eugênia. *Direito do Comércio Eletrônico*. 2. ed. Rio de Janeiro: Elsevier: 2011, p. 124-125.

2 DIREITO A PROTEÇÃO DE DADOS PESSOAIS NA LEGISLAÇÃO ESTRANGEIRA

A proteção de dados pessoais, tema que apresenta um razoável grau de maturação em diversos ordenamentos jurídicos, enfrenta barreiras formais e materiais ao seu pleno desenvolvimento no ordenamento brasileiro[5].

Lawrence Lessig[6], renomado doutrinador na área de Direito Digital, define privacidade como tudo que é resultante da subtração, de todos os aspectos da vida social, de tudo que é monitorado e de tudo que é investigado.

No atual patamar de desenvolvimento tecnológico, a informação é um dos bens mais valorosos. O aumento da eficiência nos métodos de monitoramento e investigação proporciona maior facilidade para manter, utilizar e coletar informações. Nesse âmbito, a informação é coletada invisivelmente, eficientemente e sem inconvenientes para o usuário[7]. Razão pela qual a sua proteção deve ser questão de superior relevância, merecendo a atenção do legislador.

Neste sentido, Cláudio de Lucena Neto, citando José Afonso da Silva comenta, com propriedade (Neto, 2002): "o perigo é tão maior quanto mais a utilização da informática facilita a interconexão de fichários com a possibilidade de formar grandes bancos de dados que desvendem a vida dos indivíduos, sem sua autorização e até sem seu conhecimento".

No mesmo entendimento, Doneda referencia Luís Roberto Barroso:

> Uma das distorções mais agudas do ciclo militar-autoritário no Brasil (...) foi o uso e, sobretudo, o abuso na utilização de informações que diferentes organismos armazenavam sobre pessoas. (...) envolvendo-as na política ordinária, os órgãos de segurança mergulharam em terreno pantanoso de perseguições a adversários, operando frequentemente nas fronteiras da marginalidade. A chamada comunidade de informações passou a constituir um poder paralelo e agressivo, que por vezes, sobrepunha-se ao poder político institucional, valendo-se de meios ilícitos para fins condenáveis. (Doneda, 2009).

A proteção de dados pessoais preconiza o tema da privacidade, entretanto, modifica seus elementos e aprofunda seus postulados. A existência de uma efetiva proteção dos dados pessoais é de relevância evidente, assim como também o desenvolvimento de formas de bloquear e controlar possíveis manipulações indevidas destes dados.

---

[5] DONEDA. Danilo A Proteção de Dados Pessoais no Ordenamento Brasileiro e a Ação de Habeas Data. *Democracia Digital e Governo Eletrônico.* v.1, n. 1, 2009.

[6] Lawrence Lessig é professor da Universidade de Harvard. É formado pela Universidade de Yale e foi professor das Universidades de Stanford e de Chicago.

[7] FINKELSTEIN. Maria Eugênia. *Direito do Comércio Eletrônico*. 2. ed. Rio de Janeiro: Elsevier: 2011, p.127.

2.1 A Proteção de Dados Pessoais na Europa

Minoritariamente, parte da doutrina afirma que o direito a proteção de dados pessoais teve seu nascimento já a partir do final da década de 1940, com a Declaração Universal dos Direitos do Homem de 1948, a Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais de 1953, e com o Pacto de Direitos Civis e Políticos, firmado em Nova Iorque no ano de 1966; visto que esses diplomas deram início a proteção do direito à privacidade, instituto este que engloba o direito a proteção dos dados pessoais.

Todavia, a doutrina majoritária segue a classificação evolutiva das leis de proteção de dados pessoais do austríaco Mayer-Schönberger[8], que identifica quatro diferentes gerações de leis.

As primeiras iniciativas legislativas para a tutela de dados pessoais surgiram, segundo Mayer-Schönberger, na década de 1970, com a Resolução nº 428 da Assembleia Parlamentar do Conselho da Europa, quando, ao discutir sobre a implementação de bancos de dados, foi exigido que o indivíduo não poderia ter expostas informações atinentes à sua vida privada. Ainda fazem parte da "primeira geração" o *Data Protection Act* de Hessen, também de 1970, o *Data Act* Suéco de 1973, o *Law of the State of Rhineland-Palatinate* contra o uso impróprio de dados de 1974 e a *Federal Data Protection Act* Alemã de 1977.

Na primeira geração a custódia das normas de proteção de dados não recaía sobre o indivíduo, mas, ao contrário, foram promulgadas em resposta ao crescente processamento eletrônico de dados pelos Estados e pelas grandes companhias. Seus princípios de proteção eram bastante abstratos e amplos, focalizados na atividade de processamento dos bancos de dados, e não na privacidade.

A segunda geração de leis sobre a matéria surgiu no final da década de 1970, com a *Bundesdatenschutzgesetz*, a lei federal da República Federativa da Alemanha sobre proteção de dados pessoais, de 1977, e a *Informatique et Libertées*, lei francesa de proteção de dados pessoais de 1978. As leis agora se baseavam na consideração da privacidade e na proteção dos dados pessoais como uma liberdade negativa, a ser exercida pelo próprio cidadão; criou-se um sistema que fornecia instrumentos para o cidadão identificar o uso indevido de suas informações pessoais e propor defesa direta de seus interesses.

[8] Viktor Mayer-Schönberger é Professor de Governança e Regulação da Internet no Instituto da Internet de Oxford, da Universidade de Oxford.

Surgida na década de 1980, a terceira geração de leis aperfeiçoa a tutela dos dados pessoais, que passa a acolher não apenas a liberdade de fornecer ou não seus dados pessoais, mas atenta, ainda, em garantir a efetividade dessa liberdade.

A proteção de dados passa a ser considerada como um processo mais complexo, que envolve a além da participação do indivíduo, mas também leva em consideração o contexto no qual lhe é solicitado que revele seus dados, possibilitando que se instaure meios de proteção para as ocasiões em que sua liberdade de decidir livremente é cerceada. Processo este denominado de autodeterminação informacional. Vários países europeus, como a Alemanha, a Áustria, a Noruega e a Finlândia, emendaram sua legislação para integrar o direito à autodeterminação informacional.

A autodeterminação informativa veio como forma de acréscimo às liberdades presentes nas leis de segunda geração. Entretanto, por causa dos custos (sendo estes econômicos ou sociais), a maioria da população consentia situações que não eram ideais; não haviam muitas pessoas dispostas a exercitar suas prerrogativas de autodeterminação informativa. Por esta razão, surge a quarta geração de leis com normas que entendem que o cidadão comum está em uma posição de barganha comumente fraca quando exerce o seu direito, e tentam retificar esse problema procurando fortalecer a posição do indivíduo em relação às entidades que coletam e processam seus dados reconhecendo, assim, o desequilíbrio nessa relação; reduzindo do papel da decisão individual de autodeterminação informativa – em razão do pressuposto de que determinadas modalidades de tratamento de dados pessoais necessitam de uma proteção em um grau maior (como é o caso de dados sensíveis).

Como exemplos das leis da quarta geração de Mayer-Schönberger tem-se a Diretiva 95/46/EC, que apresenta os princípios norteadores que devem ser adotados nas legislações internas dos países membros e ressalta que a proteção dos dados pessoais deve ser aplicada tanto ao tratamento automatizado de dados como ao tratamento manual, da mesma forma que a observância de suas determinações devem se dar tanto pelo setor público quanto pelo setor privado[9]; a Diretiva 2002/58/CE, que regulamenta a proteção de dados pessoais no contexto da comunicação eletrônica; apesar de tratar sobre tema já contido no ordenamento da comunidade europeia, essa Diretiva permitiu a adequação das normas contidas na Diretiva

[9] Consideração 27 da Diretiva 95/46/EC: "Whereas the protection of individuals must apply as much to automatic processing of data as to manual processing; whereas the scope of this protection must not in effect depend on the techniques used, otherwise this would create a serious risk of circumvention; whereas, nonetheless, as regards manual processing, this Directive covers only filing systems, not unstructured files; whereas, in particular, the content of a filing system must be structured according to specific criteria relating to individuals allowing easy access to the personal data (…)".

95/46/CE à realidade tecnológica atual; e a Diretiva 06/24/CE, que dispõe da guarda de dados gerados ou tratados nos provedores de serviços de comunicações eletrônicas publicamente disponíveis ou de redes públicas de comunicações, indica, ainda, que a Diretiva deverá ser aplicada ao tráfego e à localização do dado tanto de pessoas jurídicas como de pessoas físicas[10].

2.1.1. Regulamento Geral sobre a Proteção de Dados – *General Data Protection Regulation* (GDPR)

O Regulamento Geral de Proteção de Dados é um regulamento pelo qual a Comissão Europeia tenta reforçar e unificar a proteção de dados dentro da União Europeia. A proposta para a GDPR foi lançada em 25 de janeiro de 2012. Em dezembro de 2015, o Conselho e o Parlamento Europeu chegaram a acordo sobre o projeto de regulamento sobre a proteção de dados. Em 8 de abril de 2016, o Conselho adotou a sua posição em primeira leitura. O Parlamento Europeu procedeu finalmente à adoção do projeto de regulamento em 14 de abril de 2016.

O novo regime de proteção de dados da UE estende o âmbito da lei de proteção de dados da UE à todas as empresas estrangeiras de processamento de dados de residentes da UE. O acordo prevê uma harmonização dos regulamentos de proteção de dados em toda a UE, tornando mais fácil para empresas não europeias cumprir tais regulamentos, no entanto, isso vem à custa do cumprimento de um regime de proteção de dados rigoroso, com severas penalidades de até 4% do volume de negócios em todo o mundo.

A GDPR atualiza e moderniza os princípios estabelecidos na Diretiva 95/46/EC. Nomeadamente, define os direitos dos indivíduos e estabelece as obrigações dos que efetuam o tratamento dos dados e dos responsáveis por esse tratamento. Estabelece ainda os métodos que garantem a conformidade e o âmbito das sanções aplicáveis aos infratores.

O novo regulamento não se aplica ao tratamento de dados pessoais para atividades de segurança nacional ou a aplicação da lei (autoridades competentes para efeitos de prevenção, investigação, detecção e repressão de infrações penais ou de execução de sanções penais). De Acordo com a Comissão Europeia, dado pessoal é qualquer informação relativa ao indivíduo, quer se trate de sua vida privada, profissional ou pública. Pode ser qualquer coisa desde um

[10] Diretiva 06/24/CE, art. 1º: "(…) this Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network."

nome, uma foto, um endereço de e-mail, dados bancários, posts em sites de redes sociais, informações médicas, ou o endereço IP de um computador.

Um único conjunto de regras serão aplicadas a todos os estados membros da UE. Cada Estado membro estabelecerá uma autoridade supervisora independente (*Supervisory Authority* – SA) para ouvir e investigar as reclamações, sancionar as infracções administrativas, etc.

As exigências de notificação permanecem e são expandidas. Eles devem incluir o tempo de retenção dos dados pessoais e informações de contato do controlador dos dados e do responsável pela proteção de dados.

Acerca da portabilidade, a GDPR estabelece em seu artigo 18 que qualquer pessoa deve ser capaz de transferir seus dados pessoais de um sistema de processamento eletrônico para outro, sem ser impedido de o fazer pelo controlador dos dados. Além disso, os dados devem ser fornecidos pelo controlador em um formato eletrônico comumente usado.

Em suma, as principais alterações acerca da proteção de dados da UE introduzidas pela GDPR são:

- Requisitos mais rigorosos na obtenção de consentimento para o recolhimento de dados pessoais;
- Elevação da idade de consentimento para o recolhimento de dados individuais de 13 para 16 anos de idade;
- Exigência de que a empresa apague os dados quando estes não forem mais usados para a finalidade à qual foram coletados;
- Exigência de que a empresa apague os dados caso o indivíduo revogue o consentimento para o armazenamento dos mesmos;
- Exigência de que as empresas notifiquem a UE acerca de violações de dados do governo, no prazo de até 72 horas;
- Criação de um único escritório nacional para monitoramento e tratamento de reclamações interpostas sob o abrigo da GDPR;
- As empresas que movimentarem quantidades significativas de dados sensíveis ou que monitorem o comportamento de muitos consumidores serão obrigadas a designar um oficial de proteção de dados;
- Multas de até € 20 milhões ou 4% da receita global da empresa.

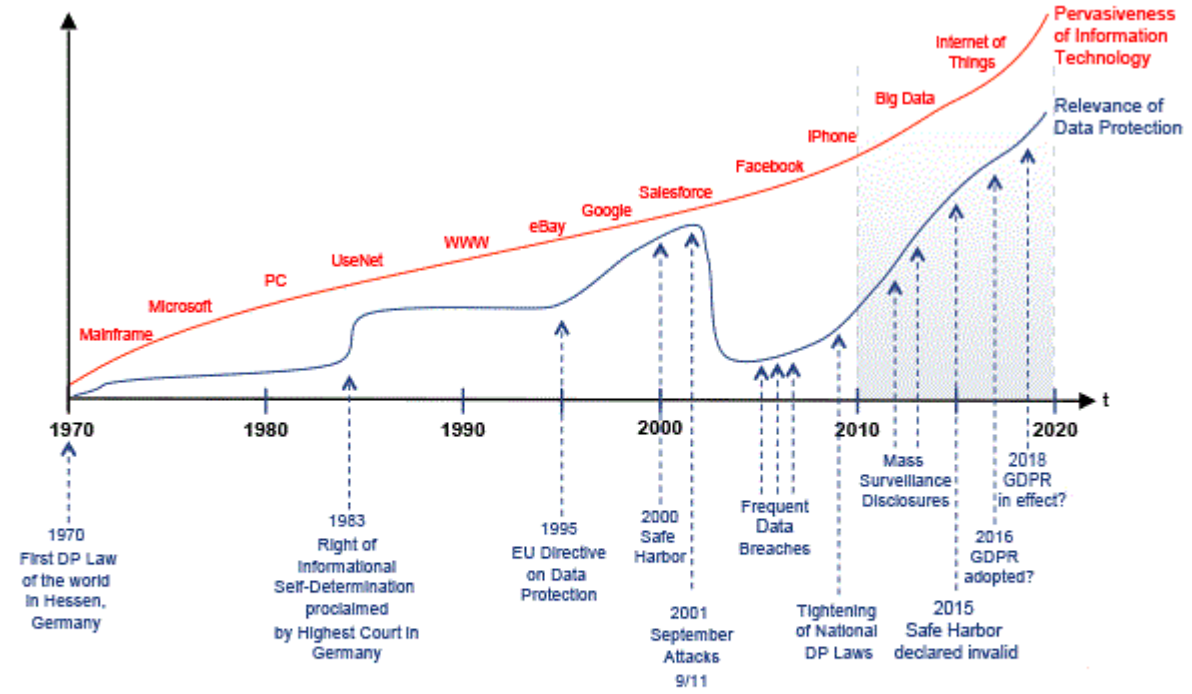

Gráfico: Relação entre a Disseminação da Tecnologia da Informação e a Relevância da Proteção de Dados.
Fonte: https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/

2.2 A Proteção de Dados Pessoais nos Estados Unidos

Ao contrário do que acontece na União Europeia, os Estados Unidos não dispõem, no momento, de legislação unificada específica sobre proteção de dados pessoais.

A legislação acerca da proteção da privacidade nos EUA tende a ser adotada numa base *ad hoc*, ou seja, o texto normativo surge quando certos setores e circunstâncias o requerem. Destarte, os EUA preferem o que chamam de uma abordagem "setorial" quanto à legislação da proteção de dados; que depende de uma combinação de legislação, regulamentação e auto-regulamentação, em contraposição a uma regulamentação única.

As mais importantes e basilares dessas leis são o *Privacy Act* de 1974 e o *Computer Matching and Privacy Act*. Essas leis são destinadas a regular exclusivamente a coleta de dados pelo governo e não tem autoridade para lidar com uso de dados pelo setor privado.

O *Computer Matching and Privacy Protection Act*, de 1988, que emendou o *Privacy Act*, protege a segurança de informações pessoais sensíveis contidas nos sistemas federais.

Há, ademais, outras leis americanas acerca do direito à privacidade e à proteção de dados. Essas leis são divididas em das categorias: a primeira lida com as informações guardadas pelo governo federal – de forma geral, essas leis contêm normas a respeito da

confidencialidade de tipos específicos de informações pessoais; e a segunda categoria se ocupa com o uso de dados pelo setor privado – a FTC[11] possui autoridade para assegurar o cumprimento de uma série de leis sobre diferentes aspectos da coleta e uso de dados de consumidores.

Diferentemente da normatização trazida pela Lei 12.965/2014 no caso da Brasil (tópico a ser analisado mais adiante neste artigo), os Estados Unidos não contam com uma previsão legal de guarda de registro de acesso a aplicações de *Internet* e de registros de conexão. Os provedores têm autonomia para decidir por quanto tempo irão manter essas informações de acordo com suas práticas comerciais e para fazer frente a eventuais processos legais.

3 DIREITO A PROTEÇÃO DE DADOS PESSOAIS NA LEGISLAÇÃO NACIONAL

Não há, no ordenamento brasileiro, legislação específica que tenha como escopo a proteção dos dados pessoais. Entretanto, tal direito, considerado internacionalmente como fundamental, não se encontra totalmente desprotegido diante da ausência legislativa.

Os princípios gerais que resguardam a proteção dos dados pessoais são, inicialmente, abarcados pela Constituição Federal de 1988, quando esta estabelece, em seu artigo 5º, os diversos direitos e garantias fundamentais dos cidadãos, e, dentre os quais, se destaca a proteção à intimidade, à privacidade e aos dados (incisos X e XII)[12].

Evidenciam-se, ainda, o Código de Defesa do Consumidor[13], que lida com questões envolvendo coleta de dados pessoais, e sua consequente armazenagem em banco de dados, envolvendo consumidores; a Lei do Cadastro Positivo[14], que disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito; e a Lei do Acesso à Informação[15], que 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, mencionando, ainda, a necessidade de

[11] Federal Trade Commission.
[12] Constituição Federal. Art. 5º: "[...] 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; [...] XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal".
[13] Lei nº 8.078/90.
[14] Lei nº 12.414/2011.
[15] Lei nº 12.527/2011.

transparência, respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.

Por fim, a proteção de dados pessoais tem sua garantia parcialmente resguardada pelo Marco Civil da Internet[16].

3.1. Marco Civil da Internet - Lei n° 12.965/2014

Em vigor desde junho de 2014, o Marco Civil traz algumas garantias gerais em relação à privacidade e à proteção dos dados pessoais.

O Marco Civil da Internet insere o tema da proteção de dados pessoais no ordenamento brasileiro. Ao estabelecer regras exigindo o consentimento do usuário para tratamento de dados, e ao permitir unicamente a coleta de dados associados, exclusivamente, com a finalidade das atividades prestadas, ratifica a necessidade de transparência nas políticas de privacidade. Reafirma, ainda, a garantia constitucional à inviolabilidade da intimidade e da vida privada, como princípio e também como direito dos usuários da rede mundial de computadores

É assegurado ao usuário a exclusão definitiva dos dados pessoais que tiver fornecido, ao término da relação entre as partes, a seu requerimento[17], a lei estabelece, também, que o acesso ao registro de conexões e a dados armazenados, de fluxo de informações e comunicações privadas somente poderá ocorrer mediante autorização judicial[18].

O Marco Civil trouxe, inegavelmente, avanços necessários na seara da proteção de dados pessoais, carente de legislação específica. Todavia, ainda há muitos pontos importantes que precisam da atenção e dos cuidados do Legislativo brasileiro, pois, por mais que a Lei 12.965/14 contenha dispositivos e princípios relacionados ao tema, estes são abordados de forma esparsa, genérica, imprecisa e incompleta.

[16] Lei 12.965/2014
[17] Lei 12.965/2014, art. 7º, X.
[18] Lei 12.965/2014, art. 13º, § 5º, e art. 15º, §3º.

4 CONSIDERAÇÕES ACERCA DO ANTEPROJETO DE PROTEÇÃO DE DADOS PESSOAIS E PRIVACIDADE

Em 2010, o Ministério da Justiça começou a elaborar um anteprojeto de lei para normatizar a proteção de dados pessoais e privacidade.

O Anteprojeto tem por objetivo garantir e proteger, no âmbito do tratamento de dados pessoais[19], a dignidade e os direitos fundamentais da pessoa, especialmente em relação à liberdade, igualdade e privacidade pessoal e familiar.

O texto proposto adota a ideia de que dado pessoal é uma informação que pode ser ligada a uma pessoa. Englobando, portanto, qualquer dado que possa ser associado a um indivíduo.

Define dados anônimos como 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 para identificar o referido titular[20]; e dados sensíveis como dados pessoais que revelem a origem racial ou étnica, as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, bem como dados genéticos[21]. Os dados sensíveis, de acordo com a proposta, devem ser protegidos de forma mais rígida.

Prevê, também, regras específicas para os setores público e privado, e critérios sobre a transferência internacional de dados.

Ademais, o Anteprojeto abarca os princípios norteadores da proteção de dados pessoais, que, além de sintetizarem os direitos e deveres estabelecidos no texto da proposta de lei, auxiliam na interpretação de seus dispositivos. Entre os princípios contidos estão, por exemplo, o princípio da finalidade, pelo qual o tratamento deve ser realizado com finalidades legítimas, específicas, explícitas e conhecidas pelo titular; o princípio da transparência e do livre acesso, segundo os quais deve ser garantida a consulta facilitada e gratuita pelos titulares sobre as modalidades de tratamento e sobre a integralidade dos seus dados pessoais e que

---

[19] Em consonância com a redação do Anteprojeto, tratamento de dados pessoais é: "o conjunto de ações referentes a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, transporte, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, bloqueio ou fornecimento a terceiros de dados pessoais, por comunicação, interconexão, transferência, difusão ou extração".

[20] Anteprojeto de Lei para a Proteção de Dados Pessoais.

[21] *Ibidem.*

essas informações devem ser dadas de forma clara e adequada; o princípio da qualidade, que assegura que os dados sejam verdadeiros e atualizados.

O capítulo VII do Anteprojeto contém padrões básicos de segurança e sigilo com procedimentos sugeridos afim de evitar possíveis vazamentos de dados e reduzir seus efeitos.

Por fim, o Anteprojeto de Lei propõe a criação de órgão administrativo específico e próprio para atuar com as questões relativas à proteção de dados pessoais.

5 CONCLUSÃO

A existência de uma efetiva proteção dos dados pessoais é de relevância evidente, assim como também o desenvolvimento de formas de bloquear e controlar possíveis manipulações indevidas destes dados.

Fruto do direito à privacidade, o direito a proteção dos dados pessoais extrapola seus limites, comunicando-se livremente com conceitos e vocábulos meta-jurídicos. Inicialmente, está contido no âmbito da privacidade, mas o supera, o abarca e o resignifica, funcionando como livre espaço de mediação. A lógica necessária ao abordar o tema, portanto, é a de que, em que pese sua denominação indique um âmbito reduzido e unilateral de estudo, seu objeto resulta numa disciplina abrangente da realidade informacional.

Para além da defesa da privacidade, o que se protege e regula, a partir de suas proposições, é o direito de acesso e o poder de controle a informações pessoais, muitas vezes que tangenciam o caráter individualista de privacidade.

Para o direito, a crescente importância que assume a necessidade de proteção dos dados pessoais se traduz no fato de que uma considerável parcela das liberdades individuais seja atualmente exercida concretamente por meio de estruturas nas quais a comunicação e a informação têm papel relevante. As diversas formas de controle tornadas possíveis com a manipulação de dados pessoais devem ser levadas em consideração pelo operador do direito.

Os juristas europeus e norte-americanos começaram a vislumbrar o potencial de dano representado pela informatização de informações pessoais já na década de 60. Na década seguinte, começaram a surgir os primeiros meios de proteção. Entendia-se que a legislação de proteção de dados pessoais deveria observar que poucos e gigantescos centros elaboradores de dados dominariam o fornecimento de informações e a gestão dos grandes bancos de dados; portanto, a ofensa à privacidade viria necessariamente destes grandes centros. Foram elaboradas leis com este fim, conhecidas pelos autores como leis de primeira geração sobre o tratamento automático de informação.

A segunda geração de leis sobre o assunto surgiu na segunda metade da década de 70, já ciente da difusão dos bancos de dados informatizados. Nelas o mecanismo de autorização para funcionamento se apresenta diluído e substituído, além de apresentarem uma melhor definição doutrinária de seus institutos. Uma terceira geração de leis, surgidas a partir da década de 80, reflete a imensa proliferação destes bancos de dados, bem como a necessidade de uma tutela flexível impossível de ser estabelecida por lei que se pretendam definitivas, dada a dinâmica do avanço tecnológico. Na quarta geração, as leis entendem que o cidadão comum está em uma posição de barganha comumente fraca quando exerce o seu direito, e tentam retificar esse problema procurando fortalecer a posição do indivíduo em relação às entidades que coletam e processam seus dados reconhecendo, assim, o desequilíbrio nessa relação.

Quanto à sistemática pátria, não há, no ordenamento brasileiro, legislação específica que tenha como escopo a proteção dos dados pessoais. Entretanto, tal direito, considerado internacionalmente como fundamental, não se encontra totalmente desprotegido diante da ausência de legislação própria; o que há, na realidade, são legislações dispersas e diferentes que trazem alguma garantia à privacidade, sem abranger o tema por completo. Entre estas, destacam-se a Lei de Cadastro Positivo, a Lei de Acesso à Informação, o Marco Civil da Internet, além de alguns dispositivos constitucionais genéricos, como os artigos 5.º, 10.º e 12.º da Constituição.

Para sanar o problema da falta de cobertura legislativa específica sobre o tema o Ministério da Justiça elaborou um anteprojeto de lei para normatizar a proteção de dados pessoais e a privacidade. O Anteprojeto faz parte do movimento nacional para os estabelecimentos de marcos regulatórios necessários em face da proliferação de novas tecnologias e, principalmente, da *Internet* no país.

Não se pode confundir, todavia, a ideia de marco regulatório com regulação. A proposição de marco vai ao encontro na natureza auto poética desse meio, ou seja, da criação intrínseca de normas de conduta, funcionando apenas como fatores limitadores de abuso, de forma a garantir a segurança jurídica a situações que recebem tratamentos diversos.

É emergente, portanto, a promulgação do Anteprojeto na forma de Lei, considerando-se que o objetivo desse texto 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 referenciado dispositivo também poderia contemplar as proteções de ordem econômica e das relações de consumo que envolvem o cidadão.

PERSONAL DATA PROTECTION:

An analysis of foreign and national legislation

ABSTRACT

The processing of personal data by automated processes is a risky activity. Considering the worldwide movement on the legal certainty and regulatory frameworks for the protection of personal data, this article analyzes the legal contours of the protection of personal data and explores its main definitions in domestic law, making a brief analysis and exposing the current situation in Brazil and analyzing the Brazilian Draft of Personal Data Protection, with the scope to outline the reality of parental rights order, and foreign law, in particular the US and the EU, tracing the origins of the right to personal data protection and its classification as a fundamental right. Using as a method raising legislation, doctrine and national and international jurisprudence and obtaining as a result the fact that Brazil currently has a dispersed and not specific protection about the personal data protection issue disposing only of mentions in chapters, articles, paragraphs and sections of different pieces of legislation and court decisions. The proliferation of new technologies and especially of the Internet in the country presses the State to the existence of legal frameworks. The Draft of Personal Data Protection objective not only the protection of personal data, but also the establishment of a legal paradigm that can serve as a bulwark for economic investment and development.

Keywords: Personal Data Protection. Privacy. Data Protection Law.

ANEXO A – ANTEPROJETO DE LEI PARA A PROTEÇÃO DE DADOS PESSOAIS

ANTEPROJETO DE LEI

Dispõe sobre o tratamento de dados pessoais para proteger a personalidade e a dignidade da pessoa natural

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

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, com o objetivo de proteger os direitos fundamentais de liberdade, intimidade e privacidade da pessoa natural.

Art. 2º Esta Lei aplica-se a qualquer operação de tratamento realizada por meio total ou parcialmente automatizado, por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do país de sua sede e do país onde esteja localizado o banco de dados, desde que:

I - a operação de tratamento seja realizada no território nacional; ou

II - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

§ 2º Esta Lei não se aplica aos tratamentos de dados:

I - realizados por pessoa natural para fins exclusivamente pessoais; ou

II - realizados para fins exclusivamente jornalísticos.

§ 3º É vedado aos órgãos públicos e entidades públicas efetuar a transferência de dados pessoais constantes de bases de dados que administram ou a que tenham acesso no exercício de suas competências legais para entidades privadas, exceto em casos de execução terceirizada ou mediante concessão e permissão de atividade pública que o exija e exclusivamente para fim específico e determinado.

Art. 3º As empresas públicas e sociedades de economia mista que atuem em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.

Parágrafo único. As empresas públicas e sociedades de economia mista, quando estiverem operacionalizando políticas públicas e não estiverem atuando em regime de concorrência, terão o mesmo tratamento dispensado aos órgãos e entidades públicas, nos termos dessa Lei.

Art. 4º Os tratamentos de dados pessoais para fins exclusivos de segurança pública, defesa, segurança do Estado, ou atividades de investigação e repressão de infrações penais, serão regidos por legislação específica, observados os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

Parágrafo único. É vedado o tratamento dos dados a que se refere o caput por pessoa de direito privado, salvo em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico ao órgão competente.

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

I - dado pessoal: dado relacionado à pessoa natural identificada ou identificável, inclusive a partir de números identificativos, dados locacionais ou identificadores eletrônicos;

II - tratamento: conjunto de ações referentes a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, transporte, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, bloqueio ou fornecimento a terceiros de dados pessoais, por comunicação, interconexão, transferência, difusão ou extração;

III - dados sensíveis: dados pessoais que revelem a origem racial ou étnica, as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, bem como dados genéticos;

IV - 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 para identificar o referido titular;

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

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

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

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

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

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

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

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

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

XIV - 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;

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

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

XVII - uso compartilhado de dados: a comunicação, a difusão, a transferência internacional, a interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos, no cumprimento de suas competências legais, ou entre órgãos e

entidades públicos e entes privados, com autorização específica, para uma ou mais modalidades de tratamento delegados por esses entes públicos; e

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

Art. 6º As atividades de tratamento de dados pessoais deverão atender aos seguintes princípios gerais:

I - princípio da finalidade, pelo qual o tratamento deve ser realizado com finalidades legítimas, específicas, explícitas e conhecidas pelo titular;

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

III - princípio da necessidade, pelo qual o tratamento deve se limitar ao mínimo necessário para a realização das finalidades almejadas, abrangendo dados pertinentes, proporcionais e não excessivos;

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

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

VI - princípio da transparência, pelo qual devem ser garantidas aos titulares informações claras e adequadas sobre a realização do tratamento;

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

VIII - princípio da prevenção, pelo qual devem ser adotadas medidas capazes de prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; e

IX - princípio da não discriminação, pelo qual o tratamento não pode ser realizado para fins discriminatórios.

§ 1º Os órgãos públicos darão publicidade às suas atividades de tratamento de dados por meio de informações claras, precisas e atualizadas em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos, respeitando o princípio da transparência disposto no inciso VI.

§ 2º O uso compartilhado de dados pessoais deve atender a finalidade específica de execução de políticas públicas e atribuição legal pelos órgãos e entidades públicas, respeitando o princípio da finalidade, adequação e necessidade dispostos nos incisos I, II e III.

CAPÍTULO II
REQUISITOS PARA O TRATAMENTO DE DADOS PESSOAIS
Seção I
Consentimento

Art. 7º O tratamento de dados pessoais somente é permitido após o consentimento livre, expresso, específico e informado do titular, salvo o disposto no art. 11.

§1º O consentimento para o tratamento de dados pessoais não pode ser condição para o fornecimento de produto ou serviço ou para o exercício de direito, salvo em hipóteses em que os dados forem indispensáveis para a sua realização.

§2º É vedado o tratamento de dados pessoais cujo consentimento tenha sido obtido mediante erro, dolo, estado de necessidade ou coação.

§3º O consentimento deverá ser fornecido por escrito ou por outro meio que o certifique.

§4º O consentimento deverá ser fornecido de forma destacada das demais cláusulas contratuais.

§5º O consentimento deverá se referir a finalidades determinadas, sendo nulas as autorizações genéricas para o tratamento de dados pessoais.

§6º O consentimento pode ser revogado a qualquer momento, sem ônus para o titular.

§7º São nulas as disposições que estabeleçam ao titular obrigações iníquas, abusivas, que o coloquem em desvantagem exagerada, ou que sejam incompatíveis com a boa-fé ou a equidade.

§8º Cabe ao responsável o ônus da prova de que o consentimento do titular foi obtido em conformidade com o disposto nesta Lei.

Art. 8º O titular de dados pessoais com idade entre doze e dezoito anos idade poderá fornecer consentimento para tratamento que respeite sua condição peculiar de pessoa em desenvolvimento, ressalvada a possibilidade de revogação do consentimento pelos pais ou responsáveis legais, no seu melhor interesse.

Art. 9º No caso do titular de dados pessoais com idade até doze anos incompletos, o consentimento será fornecido pelos pais ou responsáveis legais, devendo o tratamento respeitar sua condição peculiar de pessoa em desenvolvimento.

Art. 10º No momento do fornecimento do consentimento, o titular será informado de forma clara, adequada e ostensiva sobre os seguintes elementos:

I - finalidade específica do tratamento;

II - forma e duração do tratamento;

III - identificação do responsável;

IV - informações de contato do responsável;

V - sujeitos ou categorias de sujeitos para os quais os dados podem ser comunicados, bem como âmbito de difusão;

VI - responsabilidades dos agentes que realizarão o tratamento; e

VII - direitos do titular, com menção explícita a:

a) possibilidade de não fornecer o consentimento, com explicação sobre as consequências da negativa, observado o disposto no § 1º do art. 6º;

b) possibilidade de acessar os dados, retificá-los ou revogar o consentimento, por procedimento gratuito e facilitado; e

c) possibilidade de denunciar ao órgão competente o descumprimento de disposições desta Lei.

§ 1º Considera-se nulo o consentimento caso as informações tenham conteúdo enganoso ou não tenham sido apresentadas de forma clara, adequada e ostensiva.

§ 2º Em caso de alteração de informação referida nos incisos I, II, III ou V do caput, o responsável deverá obter novo consentimento do titular, após destacar de forma específica o teor das alterações.

§ 3º Em caso de alteração de informação referida no inciso IV do caput, o responsável deverá comunicar ao titular as informações de contato atualizadas.

§ 4º Nas atividades que importem em coleta continuada de dados pessoais, o titular deverá ser informado regularmente sobre a continuidade, nos termos definidos pelo órgão competente.

Art. 11. O consentimento será dispensado quando os dados forem de acesso público irrestrito ou quando o tratamento for indispensável para:

I - cumprimento de uma obrigação legal pelo responsável;

II - tratamento e uso compartilhado de dados relativos ao exercício de direitos ou deveres previstos em leis ou regulamentos pela administração pública;

III - execução de procedimentos pré-contratuais ou obrigações relacionados a um contrato do qual é parte o titular, observado o disposto no § 1º do art. 6º;

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

V - exercício regular de direitos em processo judicial ou administrativo;

VI - proteção da vida ou da incolumidade física do titular ou de terceiro;

VII - tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias.

§ 1º Nas hipóteses de dispensa de consentimento, os dados devem ser tratados exclusivamente para as finalidades previstas e pelo menor período de tempo possível, conforme os princípios gerais dispostos nesta Lei, garantidos os direitos do titular.

§ 2º Nos casos de aplicação do disposto nos incisos I e II, será dada publicidade a esses casos, nos termos do parágrafo 1º do art. 6º § 3º No caso de descumprimento do disposto no §2º, o operador ou o responsável pelo tratamento de dados poderá ser responsabilizado.

Seção II Dados Pessoais Sensíveis

Art. 12. É vedado o tratamento de dados pessoais sensíveis, salvo:

I - com fornecimento de consentimento especial pelo titular:

a) mediante manifestação própria, distinta da manifestação de consentimento relativa a outros dados pessoais; e

b) com informação prévia e específica sobre a natureza sensível dos dados a serem tratados, com alerta quanto aos riscos envolvidos no tratamento desta espécie de dados; ou

II - sem fornecimento de consentimento do titular, quando os dados forem de acesso público irrestrito, ou nas hipóteses em que for indispensável para:

a) cumprimento de uma obrigação legal pelo responsável;

b) tratamento e uso compartilhado de dados relativos ao exercício regular de direitos ou deveres previstos em leis ou regulamentos pela administração pública;

c) realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a dissociação dos dados pessoais;

d) exercício regular de direitos em processo judicial ou administrativo;

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias.

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

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

§ 3º Nos casos de aplicação do disposto nos itens ‘a’ e ‘b’ pelos órgãos e entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do §1º do art. 6º.

Art. 13. Órgão competente poderá estabelecer medidas adicionais de segurança e de proteção aos dados pessoais sensíveis, que deverão ser adotadas pelo responsável ou por outros agentes do tratamento.

§ 1º A realização de determinadas modalidades de tratamento de dados pessoais sensíveis poderá ser condicionada à autorização prévia de órgão competente, nos termos do regulamento.

§ 2º O tratamento de dados pessoais biométricos será disciplinado por órgão competente, que disporá sobre hipóteses em que dados biométricos serão considerados dados pessoais sensíveis.

Seção III Término do Tratamento

Art. 14. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

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

II - fim do período de tratamento;

III - comunicação do titular; ou

IV - determinação de órgão competente quando houver violação de dispositivo legal ou regulamentar.

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

Art. 15. Os dados pessoais serão cancelados após o término de seu tratamento, autorizada a conservação para as seguintes finalidades:

I - cumprimento de obrigação legal pelo responsável;

II - pesquisa histórica, científica ou estatística, garantida, sempre que possível, a dissociação dos dados pessoais; ou

III - cessão a terceiros, nos termos desta Lei.

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

CAPÍTULO III DIREITOS DO TITULAR

Art. 16. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais, garantidos os direitos fundamentais de liberdade, intimidade e privacidade, nos termos desta Lei.

Art. 17. O titular dos dados pessoais tem direito a obter:

I - confirmação da existência de tratamento de seus dados;

II - acesso aos dados;

III - correção de dados incompletos, inexatos ou desatualizados; e

IV - dissociação, bloqueio ou cancelamento de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei.

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

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

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

I - comunicar que não é agente de tratamento dos dados; ou

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

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

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

Art. 18. A confirmação de existência ou o acesso a dados pessoais serão providenciados, a critério do titular:

I - em formato simplificado, imediatamente; ou

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

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

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

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

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

§ 3º O titular poderá solicitar cópia eletrônica integral dos seus dados pessoais em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento, sempre que o banco de dados estiver em suporte eletrônico.

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

Art. 19. O titular dos dados tem direito a solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive as decisões destinadas a definir o seu perfil ou avaliar aspectos de sua personalidade.

§ 1º O responsável deverá fornecer, sempre que solicitadas, informações adequadas a respeito dos critérios e procedimentos utilizados para a decisão automatizada.

§ 2º Ficam ressalvados os tratamentos de dados pessoais necessários ao cumprimento de obrigação legal.

Art. 20. Os dados pessoais referentes a exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

Art. 21. A defesa dos interesses e direitos dos titulares de dados poderá ser exercida em juízo individual ou coletivamente, na forma do disposto na Lei no 9.507, de 12 de novembro de 1997, nos arts. 81 e 82 da Lei no 8.078, de 11 de setembro de 1990, na Lei no 7.347, de 24 de julho de 1985, e nos demais instrumentos de tutela individual e coletiva.

CAPÍTULO IV COMUNICAÇÃO E INTERCONEXÃO

Art. 22. Nos casos de comunicação ou interconexão de dados pessoais, o cessionário ficará sujeito às mesmas obrigações legais e regulamentares do cedente, com quem terá responsabilidade solidária pelos danos eventualmente causados.

Parágrafo único. A responsabilidade solidária não se aplica aos casos de comunicação ou interconexão realizadas no exercício dos deveres de que trata a Lei no 12.527, de 18 de novembro de 2011, relativos à garantia do acesso a informações públicas.

Art. 23. A comunicação ou interconexão de dados pessoais entre pessoas de direito privado dependerá de consentimento livre, expresso, específico e informado, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

Art. 24. A comunicação ou interconexão de dados pessoais entre pessoa jurídica de direito público e pessoa de direito privado dependerá de consentimento livre, expresso, específico e informado do titular, salvo:

I - nas hipóteses de dispensa do consentimento previstas nesta Lei;

II - nos casos de uso compartilhado de dados previsto no inciso XVII do art. 5º, em que será dada publicidade nos termos do §1º do art. 6º; ou

III - quando houver prévia autorização de órgão competente, que avaliará o atendimento ao interesse público, a adequação e a necessidade da dispensa do consentimento.

Parágrafo único. A autorização prevista no inciso III do caput poderá ser condicionada:

I - à comunicação da interconexão aos titulares, nos termos do §1º do art. 6º;

II - ao oferecimento aos titulares de opção de cancelamento de seus dados; ou

III - ao cumprimento de obrigações complementares determinadas por órgão competente.

Art. 25. A comunicação ou interconexão entre órgãos e entidades de direito público será objeto de publicidade, nos termos do §1º do art. 6º, e obedecerá às regras gerais deste Capítulo.

Art. 26. O órgão competente poderá solicitar, a qualquer momento, aos órgãos e entidades públicos que realizem interconexão de dados e o uso compartilhado de dados pessoais, informe específico sobre o âmbito, natureza dos dados e demais detalhes do tratamento realizado, podendo emitir recomendações complementares para garantir o cumprimento desta Lei.

Art. 27. Órgão competente poderá estabelecer normas complementares para as atividades de comunicação e interconexão de dados pessoais.

CAPÍTULO V TRANSFERÊNCIA INTERNACIONAL DE DADOS

Art. 28. A transferência internacional de dados pessoais somente é permitida para países que proporcionem nível de proteção de dados pessoais equiparável ao desta Lei, ressalvadas as seguintes exceções:

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

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

III - quando órgão competente autorizar a transferência, nos termos de regulamento;

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

V - quando a transferência for necessária para execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do §1º do art. 6º.

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

I - normas gerais e setoriais da legislação em vigor no país de destino;

II - natureza dos dados;

III - observância dos princípios gerais de proteção de dados pessoais previstos nesta Lei;

IV - adoção de medidas de segurança previstas em regulamento; e

V - outras circunstâncias específicas relativas à transferência.

Art. 29. Nos casos de países que não proporcionem nível de proteção equiparável ao desta Lei, o consentimento de que trata o art. 7º será especial, fornecido:

I - mediante manifestação própria, distinta da manifestação de consentimento relativa a outras operações de tratamento; e

II - com informação prévia e específica sobre o caráter internacional da operação, com alerta quanto aos riscos envolvidos, de acordo com as circunstâncias de vulnerabilidade do país de destino.

Art. 30. A autorização referida no inciso III do caput do art. 28 será concedida quando o responsável pelo tratamento apresentar garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular, apresentadas em cláusulas contratuais aprovadas para uma transferência específica, em cláusulas contratuais-padrão ou em normas corporativas globais, nos termos do regulamento.

§ 1º Órgão competente poderá elaborar cláusulas contratuais-padrão, que deverão observar os princípios gerais de proteção de dados e os direitos do titular, garantida a responsabilidade solidária, independente de culpa, de cedente e cessionário.

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

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

Art. 31. O cedente e o cessionário têm responsabilidade solidária pelo tratamento de dados realizado no exterior ou no território nacional, em qualquer hipótese, independente de culpa.

Art. 32. No caso de transferência internacional de dados de país estrangeiro para o Brasil, somente é permitido o seu tratamento no território nacional quando nas operações realizadas naquele país tiverem sido observadas suas normas relativas à obtenção de consentimento.

Art. 33. Órgão competente poderá estabelecer normas complementares que permitam identificar uma operação de tratamento como transferência internacional de dados pessoais.

CAPÍTULO VII RESPONSABILIDADE DOS AGENTES

Seção I Agentes do Tratamento e Ressarcimento de Danos

Art. 34. São agentes do tratamento de dados pessoais o responsável e o operador.

Art. 35. Todo aquele que, por meio do tratamento de dados pessoais, causar a outrem dano material ou moral, individual ou coletivo, é obrigado a ressarci-lo.

§ 1º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação ou quando a produção de prova pelo titular resultar excessivamente onerosa;

§ 2º O responsável ou o operador podem deixar de ser responsabilizados se provarem que o fato que causou o dano não lhes é imputável.

Art. 36. A eventual dispensa da exigência do consentimento não desobriga os agentes do tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

Art. 37. As punições cabíveis no âmbito desta Lei serão aplicadas pessoalmente aos operadores e responsáveis de órgãos públicos que agirem de forma contrária a esta Lei, conforme disposto na Lei no 8.112, de 11 de dezembro de 1990 e na Lei no 8.429, de 2 de junho de 1992.

Art. 38. As competências e responsabilidades relativas à gestão de bases de dados nos órgãos e entidades públicos, bem como a responsabilidade pela prática de atos administrativos referentes a dados pessoais, serão definidas nos atos normativos que tratam da definição de suas competências.

Seção II Responsável e Operador

Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo responsável, que verificará a observância das próprias instruções e das normas sobre a matéria.

§ 1º O responsável tem responsabilidade solidária quanto a todas as operações de tratamento realizadas pelo operador.

§ 2º Órgão competente poderá determinar ao responsável que elabore relatório de impacto à privacidade referente às suas operações de tratamento de dados, nos termos do regulamento.

Art. 40. O responsável ou o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, observado o disposto no art. 15. Parágrafo único. Órgão competente poderá dispor sobre formato, estrutura e tempo de guarda do registro.

Seção III Encarregado pelo Tratamento de Dados Pessoais

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

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente de forma clara e objetiva, preferencialmente na página eletrônica do responsável na Internet.

§ 2 o As atividades do encarregado consistem em:

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

II - receber comunicações do órgão competente e adotar providências;

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

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

§ 3º Órgão competente estabelecerá normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de definição, conforme critérios de natureza ou porte da entidade, e volume de operações de tratamento de dados.

Seção IV Segurança e Sigilo dos Dados

Art. 42. O operador deve adotar medidas de segurança técnicas e administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação, difusão, ou qualquer forma de tratamento inadequado ou ilícito.

Parágrafo único. As medidas de segurança devem ser compatíveis com o atual estado da tecnologia, com a natureza dos dados e com as características específicas do tratamento, em particular no caso de dados sensíveis.

Art. 43. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se ao dever de sigilo em relação aos dados pessoais, mesmo após o seu término.

Art. 44. O responsável deverá comunicar imediatamente ao órgão competente a ocorrência de qualquer incidente de segurança que possa acarretar prejuízo aos titulares.

Parágrafo único. A comunicação deverá mencionar, no mínimo:

I - descrição da natureza dos dados pessoais afetados;

II - informações sobre os titulares envolvidos;

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

IV - riscos relacionados ao incidente; e

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

Art. 45. Órgão competente poderá determinar a adoção de providências quanto a incidentes de segurança relacionados a dados pessoais, conforme sua gravidade, tais como:

I - pronta comunicação aos titulares;

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

III - medidas para reverter ou mitigar os efeitos de prejuízo.

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

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

Art. 46. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Art. 47. Órgão competente poderá estabelecer normas complementares acerca de critérios e padrões mínimos de segurança, inclusive com base na evolução da tecnologia.

Seção V Boas Práticas

Art. 48. Os responsáveis pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas que estabeleçam condições de organização, regime de funcionamento, procedimentos, normas de segurança, padrões técnicos, obrigações específicas para os diversos envolvidos no tratamento, ações formativas ou mecanismos internos de supervisão, observado o disposto nesta Lei e em normas complementares sobre proteção de dados.

Parágrafo único. As regras de boas práticas disponibilizadas publicamente e atualizadas poderão ser reconhecidas e divulgadas pelo órgão competente.

Art. 49. O órgão competente estimulará a adoção de padrões técnicos para softwares e aplicações de Internet que facilitem a disposição dos titulares sobre seus dados pessoais, incluindo o direito ao não rastreamento.

CAPÍTULO VIII SANÇÕES ADMINISTRATIVAS

Art. 50. As infrações realizadas por pessoas jurídicas de direito privado às normas previstas nesta Lei ficam sujeitas às seguintes sanções administrativas aplicáveis por órgão competente:

I - multa simples ou diária;

II - publicização da infração;

III - dissociação dos dados pessoais;

IV - bloqueio dos dados pessoais;

V - suspensão de operação de tratamento de dados pessoais, por prazo não superior a dois anos;

VI - cancelamento dos dados pessoais;

VII - proibição do tratamento de dados sensíveis, por prazo não superior a dez anos; e

VIII - proibição de funcionamento de banco de dados, por prazo não superior a dez anos.

§ 1º As sanções poderão ser aplicadas cumulativamente.

§ 2º Os procedimentos e critérios para a aplicação das sanções serão adequados em relação à gravidade e à extensão da infração, à natureza dos direitos pessoais afetados, à existência de reincidência, à situação econômica do infrator e aos prejuízos causados, nos termos do regulamento.

§ 3º Os prazos de proibição previstos nos incisos VII e VIII do caput poderão ser prorrogados pelo órgão competente, desde que verificada a omissão no cumprimento de suas determinações, a reincidência no cometimento de infrações ou a ausência de reparação integral de danos causados pela infração.

§ 4º O disposto neste artigo não prejudica a aplicação de sanções administrativas, civis ou penais definidas em legislação específica.

§ 5º O disposto nos incisos III a VII poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei no 8.112, de 11 de dezembro de 1990 e na Lei no 8.429, de 2 de junho de 1992.

CAPÍTULO IX DISPOSIÇÕES TRANSITÓRIAS E FINAIS

Art. 51. Órgão competente estabelecerá normas sobre adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, considerada a complexidade das operações de

REFERÊNCIAS

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Disponível em: < http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 20 abr. 2015.

_____. Lei nº 12.965, de 23 de abril de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 20 abr. 2015.

DONEDA. Danilo. A Proteção dos Dados Pessoais como um Direito Fundamental. *Espaço Jurídico.* Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

_____. A Proteção de Dados Pessoais no Ordenamento Brasileiro e a Ação de Habeas Data. *Democracia Digital e Governo Eletrônico.* v.1, n. 1, 2009.

_____. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

UNIÃO EUROPEIA. *Diretiva 95/46/EC.* Disponível em: <http://eur-lex.europa.eu/LexUriServ.do?uri=CELEX:31995L0046:en:HTML >. Acesso em 7 abr. 2015.

FINKELSTEIN. Maria Eugênia. *Direito do Comércio Eletrônico*. 2. ed. Rio de Janeiro: Elsevier: 2011.

GIL, Antonio Carlos. *Como elaborar projetos de pesquisa*. 5. ed. São Paulo: Atlas, 2008.

LAKATOS, Eva Maria. MARCONI, Marina de Andrade. *Fundamentos de metodologia científica*. 5. ed. São Paulo: Atlas 2003.

LEITE, George Salomão. LEMOS, Ronaldo. *Marco Civil da Internet*. São Paulo: Atlas, 2014.

LESSIG, Lawrence. *The Architecture of Privacy. Conferência na Taiwan Net*. Taipei. mar. 1998.

LORENZETTI. Ricardo L. Trad. Fabiano Menke. Notas de Cláudia Lima Marques. *Comércio Eletrônico*. São Paulo: Editora dos Tribunais, 2004.

MAYER-SCÖNBERGER, Viktor. "General development of data protection in Europe", in: *Technology and privacy: The new landscape*. AGRE, Phillip; ROTENBERG, Marc. (orgs.). Cambridge: MIT Press, 1997, pp. 219-242.

MICHEL, Maria Helena. *Metodologia e pesquisa científica em ciências sociais*. São Paulo: Atlas, 2005.

NETO, Cláudio de Lucena. Função Social da Privacidade. *Jus Navegandi.* 2002. Disponível em: <http://jus.com.br/artigos/2834>. Acesso em: 7 abr. 2015.

RODRIGUEZ. Danilo Piñeiro. RUARO. Regina Linden. *O Direito à Proteção de Dados Pessoais na Sociedade de Vigilância.* Trabalho apresentado na V Mostra de Pesquisa da Pós-Graduação. PUCRS, 2010.