DOI: http://dx.doi.org/10.14295/revistadaesmesc.v23i29.p165

A PROTEÇÃO DE DADOS PESSOAIS NAS RELAÇÕES DE CONSUMO COMO UM DIREITO FUNDAMENTAL: PERSPECTIVAS DE UM MARCO REGULATÓRIO PARA O BRASIL[1]

DATA PROTECTION OF PERSONAL CONSUMPTION IN RELATIONS AS A FUNDAMENTAL RIGHT : PROSPECTS OF A REGULATORY FRAMEWORK FOR BRAZIL

Larissa Britto Florenço[2]

Resumo: Este artigo objetiva analisar quais instrumentos normativos são oferecidos quanto à proteção de dados pessoais nas relações de consumo no Brasil e a perspectiva da instituição de marco regulatório na matéria. Por meio de um sistema dedutivo, almeja-se evidenciar a tratativa que possui a matéria na legislação brasileira e se a instituição de uma nova dinâmica normativa será eficiente nos objetivos a que se destina. Para tanto, evidencia-se, inicialmente, que a matéria adquirira *status* constitucional, assim como patamar de direito fundamental. Ainda, verifica-se que, com o alto desenvolvimento tecnológico aliado ao mercado capitalista que se vivencia, diversas normativas surgiram no decorrer dos últimos anos a fim de resguardar os dados pessoais propagados pelos indivíduos. Aborda-se que, em comparativo com a legislação de que tratam o tema em outros países, o Brasil oferece proteção em legislações esparsas, mas não concede medida profilática para o uso indevido de dados pessoais. Constata-se que, embora haja a perspectiva de lei que regule a matéria no país, o projeto teve por base a legisla-

1 O presente artigo, adaptado para este fim, é fruto de Trabalho de Conclusão de Pós-Graduação em Direito Aplicado orientado pelo Dr. Cláudio Eduardo Régis de Figueiredo e Silva e submetido à banca examinadora da Universidade Regional de Blumenau (FURB) como requisito à obtenção do título de especialista no ano de 2015.

2 Pós-Graduada em nível de especialização em Direito Aplicado em curso promovido pela FURB em parceria com a Escola Superior da Magistratura do Estado de Santa Catarina. Bacharela em Direito pela Universidade do Sul de Santa Catarina (Unisul). Residente Judicial no gabinete da 2ª Vara Cível da Comarca da Capital – Foro Distrital do Continente. E-mail: larissabrittof@hotmail.com

ção europeia, cuja existência já possui mais de quinze anos e está a iminência de reforma para reaver situações que com a experiência não obtiveram bons resultados. Ao fim, conclui-se que ainda será papel do Poder Judiciário na resolução dos conflitos concernentes à matéria, mesmo que a nova dinâmica que está para ser adotada no Brasil signifique um grande passo para acompanhar a movimentação das legislações internacionais.

Palavras-chave: Privacidade. Proteção de dados. Dados pessoais. Consumidor. Marco regulatório.

Abstract: This article aims to analyze which regulatory instruments are offered for the protection of personal data in consumer relations in Brazil and the perspective of regulatory institution in the field. Through a deductive system, aims to highlight the dealings that has the matter in the Brazilian legislation and the establishment of a new regulatory dynamics will be efficient in the objectives it is designed. Therefore, it became clear initially that the matter had acquired constitutional status, as well as a fundamental right level. Still, it was found that with the high technological development coupled with the capitalist market that we experience, several regulations have emerged over the past years in order to protect the personal data propagated by individuals. If approached that in comparison with the legislation that treat the subject in other countries, Brazil provides protection in scattered legislation, but does not grant a prophylactic measure to the misuse of personal data. It was found that, although there is the law of perspective governing the matter in the country, the project was based on European law, the existence of which already has more than fifteen years and is about to reform to recover situations that the experience did not get good results. In the end, it was concluded that it will still be role of the judiciary in resolving conflicts concerning the matter, even if the new dynamic that is to be adopted in Brazil means a big step to track the movement of international law.

Keywords: Privacy. Data protection. Personal data. Consumer regulation.

1 INTRODUÇÃO

A sociedade vivencia um avançar tecnológico em que os dados pessoais, especialmente os dados pessoais dos consumidores, passaram a ser atraentes ao mercado, que os utilizam para diversos fins e os deixam de certa forma vulneráveis.

Essa nova roupagem apresenta riscos e a defesa do consumidor, em face da desenfreada propagação de seus dados, estará incumbida de proporcionar respostas a tal gravame ao fornecer proteção contra a utilização abusiva dessas informações por meio de instrumentos garantidores, limitadores e

transparentes quantos à divulgação dos dados pessoais.

É crescente a preocupação das normativas atuais acerca do tema de proteção de dados pessoais, principalmente no que tange à propagação de informações de consumidores em bancos de dados, tanto que a matéria adquirira o status de direito fundamental, pois diretamente relacionada aos direitos de personalidade de proteção da privacidade, intimidade e vida privada.

Não existe normativa específica sobre proteção de dados pessoais no Brasil, mas há proteção constitucional e outros instrumentos fornecidos por meio de leis esparsas, como os mecanismos oferecidos no Código de Defesa do Consumidor. Todavia, tal ausência fora observada, estudada, discutida em plataforma virtual oferecida pelo Ministério da Justiça e, atualmente, encontra – se a iminência de ser aprovada lei que protege a privacidade e dados pessoais – marco normativo na proteção de dados pessoais.

Assim, a questão que se buscará responder é: a lei acerca da proteção de dados pessoais que tramita no Congresso Nacional oferecerá meios efetivos de resguardos e limites a que se propõe aos dados pessoais e fundamentais dos consumidores?

Para solucionar tal questionamento, inicialmente, contextualizar-se-á o leitor, de forma sucinta e sem a presunção de esgotar o assunto, acerca da conjuntura dos dados pessoais do consumidor como um direito fundamental, as principais normativas no âmbito mundial em que envolve a matéria, assim como os instrumentos regulatórios que o país possui.

Por fim, após as breves considerações dos pontos supra referidos, buscar-se-á, finalmente, fazer uma análise dos principais tópicos do projeto de lei de proteção de dados pessoais brasileiro, cuja normativa fará o país acompanhar as principais tendências mundiais quanto ao assunto.

2 O RECONHECIMENTO DE DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

Sob as modernas condições de processamento de dados, a inviolabilidade da intimidade e da vida privada pressupõe a proteção do indivíduo contra a coleta, o armazenamento, o uso e a transmissão irrestrita de seus dados pessoais. Essa proteção é abrangida pelo direito fundamental do art. 5º, X, c/c o art. 5º, LXXII, da Constituição Federal (CF/88), à luz do princípio da dignidade da pessoa humana, de modo que atribui ao cidadão de controlar livremente a divulgação, transmissão e uso de seus dados pessoais, bem como garante o tratamento leal e lícito dos seus dados, conforme o princípio da boa – fé objetiva e da proteção das suas legítimas expectativas (MENDES, 2014, p. 235).

O problema ocorre quando a coleta de dados sobre consumidores, sem a menor filtragem e sem levar em consideração se tratar de dado sensível ou não, estão sendo utilizados como objetos de interesses por diversas empresas, para, muitas vezes, oferecer especificamente publicidade comportamental *(behavioraladvertising)* e influenciar os consumidores em suas escolhas (DONEDA, 2010, p. 62).

Doneda (2010, p. 17) ainda ressalta que na atualidade a informação pessoal é considerada uma verdadeira mercadoria em torno da qual surgem novos modelos de negócios que procuram extrair valor monetário do intenso fluxo de informações pessoais proporcionado pelas modernas tecnologias de informação. A informação pessoal, portanto, passo a ser um verdadeiro bem jurídico e / ou econômico.

Diversas ferramentas foram criadas com a finalidade de obter essas informações, capazes de coletar e compartilhar dados relacionados aos usuários e seu cotidiano, por meio da computação pervasiva (*pervasivecomputing)*[3] ou se utili-

3 *Pervasive computing* nada mais é que a integração no cotidiano das pessoas e no

zando de mecanismos como *Tracking cookie*[4], *Data Mining*[5], *Spam*[6], *Cookies*[7] entre outros.

O tratamento generalizado dos dados pessoais pelo setor privado para segmentar produtos e serviços e aumentar a eficiência de seu processo produtivo, ampliam-se as ameaças à personalidade do consumidor e os riscos de sua discriminação e estigmatização de mercado (MENDES, 2014, p. 236).

Conforme entendimento de Mendes (2014, p. 236), a concretização do dever estatal de proteção do consumidor (art. 5º,

---

seu ambiente que as circundam, de ferramentas de comunicação capazes de coletar informações durante todo o seu uso. Tais ferramentas são largamente usadas e úteis no monitoramento de atividades, sistemas de transportes inteligentes etc (VAZQUEZ apud REINO UNIDO, 2006).

4 *Tracking cookie* é um arquivo de texto. Cada cookie consegue rastrear o que o usuário faz na internet e estas informações são utilizadas de maneira compartilhada entre os sites. Assim, quando o usuário acessa determinado site, a própria página fará uma série de leitura das informações contidas no trancking cookies, adicionando ao seu banco. O objetivo ao fazer isso é conseguir reunir sobre o comportamento do internaurta oferecendo a este usuário promoções e produtos que estão de acordo com o gosto pessoal dele. Outra utilização do trancking cookies é a captura de informações relativas a bancos e cartões de crédito. Assim, quando a pessoa vai fazer uma compra online, alguns dados são preenchidos automaticamente (Novaes, 2013).

5 *Data Mining* é o processo de descobrir informações relevantes, como padrões, associações, mudanças, anomalias e estruturas, em grandes quantidades de dados armazenados em banco de dados, depósitos de dados ou outros repositórios de informação. Devido a disponibilidade de enormes quantias de dados em formas eletrônicas, e a necessidade iminente de extrair delas informações e conhecimento úteis a diversas aplicações, por exemplo na análise de mercado, administração empresarial, apoio à decisão, *data mining* foi popularmente tratado como sinônimo de descoberta de conhecimento de base de dados (Disponível em: http://www.dct.ufms.br/~mzanusso/Data_Mining.htm).

6 *Spam* é o termo utilizado para referir-se aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, esse tipo de mensagem é chamada de UCE (do inglês *UnsolicitedCommercial E-mail*) (Disponível em: http://www.antispam.br/conceito/).

7 Os *cookies* são arquivos de internet que armazenam temporariamente o que o internauta está visitando na rede. Esses byes geralmente possuem formato de texto e não ocupam praticamente nenhum espaço no disco rígido do computador. Não há limite para quais informações os cookies podem armazenar. Eles são capazes de registrar um endereço de e-mail, as preferências de pesquisa no Google, a cidade de onde você mora e muito mais. E é justamente essa capacidade de registro que pode tornar o cookie um grande vilão da internet, se for usado com objetivos ruins, como no caso de armazenar login e senhado usuário, de forma que ele não precise escrever tudo novamente quando voltar, tornando-se um perigo quando o computador é compartilhado com outros usuários, pois não terão dificuldade em acessar as páginas em que a senha está registrada. Junto com as informações guardadas, os cookies também conseguem registrar quais sites o usuário acessou enquanto navegava, expondo a privacidade do internauta para outras pessoas (disponível em: http://seguranca.uol.com.br/antivirus/dicas/curiosidades/o-que-sao-cookies-e-como-eles-podem-me-prejudicar.html#rmcl).

XXXII, da CF/88) numa sociedade caracterizada pelo amplo fluxo de informações, somente pode ser atingida com o reconhecimento de um direito básico do consumidor à proteção de dados pessoais.

Os dados pessoais, portanto, são a pessoa e como tal devem ser tratados, justificando o recurso ao instrumento jurídico destinado à tutela da pessoa e afastando a utilização de um regime de livre apropriação e disposição contratual destes dados que não levam em conta seu caráter personalíssimo (DONENA, 2010, p. 52).

3 NORMATIZAÇÃO DA PROTEÇÃO DE DADOS PESSOAIS

Há diversos ordenamentos jurídicos que reputam os dados pessoais como um direito fundamental na atualidade – uma verdadeira chave para efetivar a liberdade da pessoa nos meandros da Sociedade da Informação[8] (DONEDA, 2010, p. 52).

No caso da proteção de dados pessoais Doneda (2010, p. 52) expõe que, com a experiência, demonstrou-se a necessidade de técnicas de tutela muito mais específicas do que as presentes no arcabouço clássico dos direitos à personalidade, seja pela complexidade técnica que exige a matéria, ou seja pelo fato de que o processamento de dados pessoais, quase sempre, é transitado longe dos olhos do seu titular.

Em recente pesquisa conduzida pela GMI[9], divisão da Lightspeed Research, fornecedor líder de soluções baseadas em tecnologia e resposta online para pesquisa de mercado glo-

8 Segundo Luís Manuel Borges Gouveia, "A Sociedade da informação está baseada nas tecnologias de informação e comunicação que envolvem a aquisição, o armazenamento, o processamento e a distribuição da informação por meios electrónicos, como a rádio, a televisão, telefone e computadores, entre outros. Estas tecnologias não transformam a sociedade por si só, mas são utilizadas pelas pessoas em seus contextos sociais, económicos e políticos, criando uma nova comunidade local e global: a Sociedade da Informação" (GOUVEIA apud ANTUNES, 2008).

9 Global Market Insite.

bal, em que foram recolhidas mais de 5.000 respostas de consumidores em toda América Latina no mês de abril de 2015, constatou-se que a violação de dados preocupa e, muito, ao consumidor latino – americano. Tanto que 76% se mostraram inseguros quanto a ter suas informações pessoais violadas, mas, ao mesmo tempo, esses usuários admitem que não estão tomando as preocupações necessárias para protegerem suas informações[10] (LOBO, 2015).

Embora na atualidade tal dinâmica da proteção de dados pessoais passou a ser discutida com mais ênfase, foi com a *privacy* americana que se pode localizar a origem da proteção à privacidade na *Common Law*, num artigo publicado por dois advogados, Samuel D. Warren e Louis D. Brandeis (1890), na *Harvard Law Review*, intitulado *The rightofprivacy,* cujo texto, além de descrever os direitos fundamentais à honra e à imagem, salientava que, se a propriedade em sentindo estrito tem que ser preservada, os fatos relativos à vida privada também, de modo que tal infração constituiria ato ilícito, alcançando o direito à propriedade o patamar de propriedade intangível (BRANDEIS et al., 1890).

10 No Brasil, em particular, os consumidores mostraram pouca confiança nas instituições para proteger informações pessoais. Em uma escala de 1 a 5, sendo 1 = completamente confiável e 5 = nada confiável, os consumidores foram questionados o quanto eles confiavam em vários provedores comerciais e outras instituições para proteger suas informações. A pesquisa constatou ainda que:Apenas 25% dos consumidores confiam plenamente em seus médicos; Apenas 23% confiam plenamente em seus bancos pessoais; Apenas 10% confiam plenamente em seus prestadores de convênio médico; Apenas 15% confiam completamente em suas empresas de cartão de crédito; Apenas 14% confiam plenamente em seus empregadores; E apenas 6% confiam completamente em varejistas. "O fato de 64% dos consumidores pesquisados na América Latina terem afirmado que não estariam dispostos a fazer negócios com empresas que tiveram violações/vazamento de dados deixa claro que eles esperam que as organizações tomem medidas adicionais para proteger suas informações para que eles não precisem fazê-lo", disse Pedro Paixão, vice-presidente de vendas internacionais para Fortinet na América Latina. A pesquisa constatou ainda que: 54% dos consumidores não estão confiantes de que suas informações pessoais estão seguras ao utilizar meios de comunicação social; 62% dos consumidores acreditam que o seu computador pessoal (desktop ou laptop, por exemplo) representa o maior risco de vazamento de dados; 22% dos consumidores acreditam que smartphones representam o maior risco; Apenas 2% cogitam a possibilidade de ameaças em dispositivos como Smart TVs ou sistemas de videogame, mostrando que os consumidores brasileiros ainda não estão bem informados sobre as questões de segurança em torno da chamada Internet das Coisas (LOBO, 2015).

Quase um século após, em 1981, o Conselho da Europa aprovou a Convenção 108 sobre a proteção de dados pessoais em processos automatizados, culminando na aprovação da Diretiva 46/95, em 1995, que inspira a maioria das legislações vigentes relacionadas à matéria de proteção de dados.

Desde então, a proteção de dados pessoais passou a ser instrumento essencial à proteção da pessoa humana em diversos ordenamentos jurídicos.

Contudo, a matéria auferiu notoriedade com a Carta dos Direitos Fundamentais da União Europeia, proclamada em 07 de dezembro de 2000, cujo art. 8º tratava da proteção de dados pessoais[11], inspirando-se no art. 8º da Convenção de Strasbourg, na Diretiva 95/46/CE e no art. 286 do Tratado da União Europeia, consolidando a técnica utilizada pelo legislador e pela doutrina de vários países europeus de considerar a tutela dos dados pessoais como um direito autônomo em relação à tutela da privacidade (DONEDA, 2010, p. 48-49).

No Brasil, a proteção de sigilo de dados dos cidadãos é uma preocupação no ordenamento jurídico, já que possui *status* constitucional, tendo em conta o art. 5º, XII, da Constituição Federal, estabelecer que é inviolável o sigilo à correspondência e às comunicações telegráficas, de dados e das comunicações telefônicas, salvo determinação judicial (KHOURI, 2013, p. 18).

Como meio célere de proteger os cidadãos, o *habeas data* está entre as garantias protegidas pelo art. 60, §4º, IV, da CF/88, tornando-a cláusula pétrea, intocável por qualquer tipo de revisão constitucional que se pretenda executar (Ruaro et al., 2011, p. 58).

11 Art. 8º. Proteção de dados pessoais. 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente (2000/C 364/01).

No plano infraconstitucional, no país, o fundamento do direito básico do consumidor à proteção de dados pessoais é o próprio Código de Defesa do Consumidor, que, a partir de suas normas principiológicas e abertas, mostra-se capaz de recepcionar as novas demandas sociais, aliado à interpretação dialógica entre o Código Civil, a Lei de Cadastro Positivo e a Lei de Acesso à Informação (MENDES, 2014, p. 236).

O reconhecimento da proteção de dados como um direito autônomo e fundamental, portanto, não deriva de uma dicção explícita e literal, infere-se da consideração dos riscos que o tratamento automatizado traz à proteção da personalidade à luz das garantias constitucionais de igualdade substancial, liberdade e dignidade pessoal humana, juntamente com a proteção da intimidade e da vida privada (DONEDA, 2010, p. 49).

4 PERSPECTIVA DE MARCO REGULATÓRIO NA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

As explanações anteriores confirmam que, contrariamente à legislação europeia, extrai-se da leitura do sistema jurídico brasileiro uma estrutura normativa complexa e não unitária, que apresentam diversos institutos esparsos (Ruaro et al., 2011, p. 56).

O Supremo Tribunal Federal (STF), em decisão relatada pelo Ministro Sepúlveda Pertence, tendo como base a tese de Tércio Sampaio Ferraz Júnior,[12] reconheceu expressamente

12 [...] o sigilo, no inciso XII do art. 5.°, refere-se à comunicação, no interesse da defesa da privacidade. Isto é feito, no texto, em dois blocos: a Constituição fala em sigilo "da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas". Note-se, para a caracterização dos blocos, que a conjunção e une correspondência com telegrafia, segue-se uma vírgula e, depois, a conjunção de dados com comunicações telefônicas. Há uma simetria nos dois blocos. Obviamente o que se regula é comunicação por correspondência e telegrafia, comunicação de dados e telefonia. O que fere a inviolabilidade do sigilo é, pois, entrar na comunicação alheia, fazendo com que o que devia ficar entre sujeitos que se comunicam privadamente passe ilegitimamente ao domínio de um terceiro. Ou seja, a inviolabilidade do sigilo garante, numa sociedade democrática, o cidadão contra a intromissão clandestina ou não autorizada pelas partes na comunicação entre elas, como, por exemplo, censura de correspondência, a figura do hacker etc. Por

que os dados armazenados na memória do computador não têm direito ao sigilo da proteção que a Constituição reserva à correspondência, sustentando que a Lei Maior protege somente a troca de dados e não os dados em si, de forma que os dados contidos em computador não estão protegidos pela lei (RE 418416, Relator(a): Min. SEPÚLVEDA PERTENCE, Tribunal Pleno, julgado em 10/05/2006, DJ 19-12-2006 PP-00037 EMENT VOL-02261-06 PP-01233).

No final do ano de 2014, a 2ª Seção do Superior Tribunal de Justiça (STJ) julgou Recurso Repetitivo (REsp 1.419.697) que tratou da consolidação do entendimento da corte sobre a natureza do sistema *scoring*, da suposta violação a princípios e regras do CDC e do cabimento de indenização por dano moral (CONJUR, 2015).

Os ministros concluíram na ocasião que o sistema é legal, mas devem ser respeitadas a privacidade e a transparência na avaliação do risco de crédito. E, apesar de ser desnecessário o consentimento do consumidor para a operação do sistema, deve haver o esclarecimento das informações pessoais valoradas (CONJUR, 2015).

De acordo com a 2ª Seção, não se pode exigir o prévio e expresso consentimento do consumidor avaliado, pois o sistema é um modelo estatístico sem a natureza de cadastro ou banco de dados. Quando solicitado, deve haver indicação clara da fonte utilizada para que o afetado possa exercer controle acerca da veracidade dos dados (CONJUR, 2015).

São inúmeros os julgados nos Tribunais brasileiros acerca do tema, tentado decidir a melhor forma como se tratar a in-

outro lado, se alguém elabora para si um cadastro sobre certas pessoas, com informações marcadas por avaliações negativas, e o torna público, poderá estar cometendo difamação, mas não quebra sigilo de dados. Se estes dados, armazenados eletronicamente, são transmitidos, privadamente, a um parceiro, em relações mercadológicas, para defesa do mercado (banco de dados), também não estará havendo quebra de sigilo. Mas se alguém entra nesta transmissão, como um terceiro que nada tem a ver com a relação comunicativa, ou por ato próprio ou porque uma das partes lhe cede o acesso sem o consentimento da outra, estará violado o sigilo de dados (FERRAZ JR. 2011).

formação pessoal e a ponderação de interesses, diante do hiato que se encontra na nossa legislação entre a tutela da privacidade, constitucionalmente prevista, da tutela das informações pessoais, cuja legislação explícita é ausente no ordenamento jurídico brasileiro (DONEDA, 2010, p. 55).

A par da atual realidade, após consulta pública proposta pelo Ministério da Justiça, fora elaborado projeto de lei sobre proteção, tratamento e o uso dos dados pessoais que já avançou no Senado e foi aprovado pela Comissão de Ciência e Tecnologia (CCT) em 13/10/2015 e, atualmente, o texto segue à Comissão de Meio Ambiente, Defesa do Consumidor, Fiscalização e Controle, embora o texto esteja altamente influenciado pela Diretiva 95/46 (DPD) Europeia.

A criação no Projeto de Lei de uma autoridade de proteção de dados, nomeada como Autoridade de Garantia, a criação de códigos de boas práticas e a vedação da transferência de dados pessoais para países estrangeiros que não dispuserem de um nível de proteção adequada, também são mecanismos semelhantes aos que se encontram da legislação europeia, inclusive a categorização de dados sensíveis (VAZQUEZ, 2012).

Sobre a similitude de alguns aspectos do projeto de lei brasileiro de proteção de dados e a legislação europeia, Vazquez (2012) faz as seguintes considerações:

> À luz da proposta inicial, é possível perceber que foram transpostos para o anteprojeto alguns dos problemas que levaram à proposta de reforma da diretiva europeia de proteção de dados. Entre os aspectos principais, é possível destacar que o anteprojeto possui o mesmo defeito encontrado na DPD, isto é, uma legislação que busca informar o "como fazer" e não qual o padrão a ser alcançado. Também não houve a menção às cláusulas contratuais modelo para a transferência internacional de dados, altamente importantes no âmbito de aplicação da DPD. Vale ressaltar que esses dois aspectos contam na pauta principal da reforma da diretiva europeia e, uma vez que o anteprojeto brasileiro está

> claramente inspirado em tal diretiva, maior atenção deveria ser dada aos problemas existentes naquela legislação, existente há mais de 15 anos.

Insta a mencionar que no ano de 2015, a própria União Europeia passou a discutir lei que endurece regras sobre privacidade de dados, alterando a maneira como as empresas estrangeiras, principalmente as americanas, lidam com os dados do consumidor na Europa. Os usuários de sites e serviços como Twitter, Google e Facebook, conforme discussão de novo projeto de lei europeu, terão de consentir explicitamente para que as empresas possam compartilhar seus dados pessoais, obrigando a remoção de links com informações pessoais excessivas ou irrelevantes dos resultados dos mecanismos de busca na internet. Assim, o objetivo seria criar uma nuvem nacional do resto, fazendo com que as informações transmitidas pela internet pertencentes à Europa deverão ser armazenadas no próprio continente (TIINSIDEONLINE, 2015).

O projeto de lei brasileiro de proteção de dados pessoais, antes mesmo de se apresentar em consulta pública, corrigiu falhas em publicação anterior, passando a apresentar-se como: "Dispõe sobre o tratamento de dados pessoais para proteger a personalidade e dignidade da pessoa natural", abarcando, assim, todos os direitos de personalidade passíveis de serem infringidos, inclusive, a intimidade (BRASIL, 2015).

Outro aspecto relevante do projeto de lei está na necessidade de consentimento na utilização de dados pessoais, de modo que, para fornecer o consentimento, o titular deve ser informado de forma ostensiva sobre a finalidade e período de uso, como ele se dará e o âmbito de sua difusão, podendo, o titular, revogar tal consentimento a qualquer tempo e sem qualquer cobrança, merecendo destaque o consentimento específico para o uso de dados sensíveis e dados de crianças[13] (FERREIRA FILHO et

13 Art. 7º: O tratamento de dados pessoais somente é permitido após o consentimento

al., 2015). Também, passou a fixar prazos máximos a ser estabelecidos por órgão competente na guarda de dados pessoais em bancos de dados[14].

No entanto, o projeto de lei é criticado por empresas que utilizam o sistema de internet em suas atividades, principalmente no que concerne ao consentimento do titular dos dados, afirmando ser inviável tal consentimento do usuário para diversas atividades da relação com o consumidor (CONJUR, 2015).

Outra problemática que também poderá surgir no texto legal, se for aprovado como se propõe, é o previsto atualmente

livre, expresso, específico e informado do titular, salvo 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 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 estabeleça, 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. 9º: No caso do titular de dados pessoais com idade de 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. 12. É vedado o tratamento de dados pessoais sensíveis, salvo: I – com fornecimento de consentimento pelo titular; a) mediante manifestação de consentimento 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 [...]. (Anteprojeto de Lei de Proteção de Dados Pessoais).

14 Art. 14. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses: [...] Parágrafo Único: O 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.

no art. 2º, §2º, inciso II,[15] que exclui do seu âmbito os bancos de dados para fins jornalísticos, que, segundo Ruaro e outros, "tal previsão está atrelada ao direito fundamental à liberdade de expressão e, por conseguinte, liberdade de imprensa". (RUARO et al., 2011, p. 62).

Para Gilmar Mendes, o texto Constitucional não exclui a possibilidade de que se introduzam limitações ao direito fundamental à liberdade de expressão e de comunicação, salientando que tais direitos devem respeitar aos demais dispositivos constitucionais, "pois, do contrário, outros valores igualmente relevantes, quedariam esvaziados diante de um avassalador, absoluto e insuscetível de restrição" (1994, p. 298).

No Anteprojeto de lei brasileiro de proteção de dados, em que pese estar previsto uma autoridade administrativa competente para a proteção de dados com diversas funções já definidas (como a competência para receber e analisar denúncias e para estabelecer parâmetros se segurança e prazos para tratamento e conservação de dados pessoais), ainda não se sabe se o órgão será de competência atribuída a alguma entidade já existente ou se haverá criação de algum agente próprio (FERREIRA FILHO et al., 2015)[16].

Sabe-se, no entanto, que a própria natureza da disciplina de

15 Art. 2º. Esta lei aplica-se a qualquer operação de tratamento realizado por meio total ou parcialmente automatizado, por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do país onde esteja localizado o banco de dados desde que: [...] §2º Esta lei não se aplica aos tratamentos de dados: [...] II – realizados para fins exclusivamente jornalísticos (BRASIL, 2015).

16 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. 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: [...] (Anteprojeto de Proteção de Dados Pessoais).

proteção de dados pessoais deverá atingir um equilíbrio entre as liberdades e direitos individuais tutelados por meio da proteção de dados pessoais e da garantia da circulação da informação necessária às relações comerciais, tal equilíbrio, de qualquer forma, se dará somente por intermádio do Poder Judiciário, legitimado na aplicação do princípio da proporcionalidade, pelo qual se avaliam os interesse em questão, procurando tutelar o conteúdo essencial do direito à privacidade, ao mesmo tempo em que se leva em conta a necessidade da utilização dos dados pessoais no caso concreto (GONÇALVES, 1994, p. 96).

5 CONCLUSÃO

A propagação do mercado e o fomento de novas tecnologias, principalmente com o avanço da internet e o uso do computador e *smartphones* cada vez mais habitual, faz-se necessário a particularização de conceitos como privacidade e intimidade diante da propagação acelerada de dados pessoais de um indivíduo.

Diante das discussões que o tema enfrenta, principalmente no que toca a proteção dos dados pessoais dos consumidores em face dos banco de dados criados pelos fornecedores ou prestadores de serviços com o fim de estratégias mercadológicas, surgiu a necessidade de regulamentação, na tentativa de obstar a liberdade absoluta e gratuidade no manuseio dos dados privados.

A tutela da proteção de dados possui fundamento constitucional e assume a feição de um direito fundamental, posto que se destina à proteção da pessoa perante interesses provindos de uma multiplicidade de fontes, sejam aquelas situadas na esfera privada como na pública, chegando, hoje, a se projetar como um direito autônomo e que necessita de uma tutela ampla e genérica (DONEDA, 2010, p. 110).

O Brasil vem enfrentando a questão por meio de instru-

mentos esparsos, a partir de interpretação dialógica das diversas normas que abordam o tratamento de dados pessoais, ganhando destaque o Código de Defesa do Consumidor. Todavia, a problemática consiste no fato de que os mecanismos oferecidos na normativa brasileira não estão sendo suficientes para a proteção da propagação desses dados, atuando somente como um remédio para o dado já propagado, ante a ausência de qualquer medida profilática ou qualquer outro meio de prevenção.

Com o objetivo de suprir falhas, está em tramite para aprovação projeto de lei sobre a proteção, tratamento e o uso de dados pessoais, cujo texto responsabiliza agentes envolvidos no armazenamento, tratamento e transferência dos dados, bem como o direito de requerer a exclusão dos dados pessoais armazenados. No entanto, além de estar fortemente baseado na Diretiva Europeia 95/46, cujo modelo possui mais de quinze anos e se encontra em processo de reforma, a norma não regula banco de dados do Estado para defesa nacional e segurança pública, assim como os de uso jornalístico e os dados para fins particulares não econômicos.

Também ausente menção de vigilância dos atos dos responsáveis pelo processamento de dados, de modo a observar se estão em consonância ou não com esse direito fundamental. Observar, vigiar e publicizar essas condutas propicia a transparência necessária para identificação das práticas que violam a Constituição e auxilia no seu combate (MENDES, 2014, p. 238).

Por conseguinte, embora haja riscos do projeto de lei de proteção e dados pessoais propagarem no âmbito nacional problemas que foram identificados nas legislações estrangeiras, será um grande passo na normativa brasileira para efetivar um direito já considerado fundamental e acompanhar a dinâmica mundial na questão do tratamento de dados privados, facilitando, inclusive, o próprio comercio exterior.

No entanto, caberá ainda ao Código de Defesa do Consumi-

dor e normas esparsas operacionalizar por procedimentos específicos acerca do tratamento dos dados pessoais, assim como continuará a tarefa ao Poder Judiciário de prestar a jurisdição quanto à ponderação dos direitos fundamentais em conflito.

REFERÊNCIAS

2000/C 364/01. *Carta dos Direito Fundamentais da União Europeia.* Disponível em: <http://www.europarl.europa.eu/charter/pdf/text_pt.pdf>. Acesso em: 12 maio 2015.

ANTUNES. Ana Maria Pereira. *Sociedade da informação.* Trabalho realizado no âmbito da disciplina de Fontes de Informação Sociológica da Licenciatura em Sociologia. Coimbra, 2008.

AS DUAS ÚLTIMAS DÉCADAS. Disponível em: <http://www.dct.ufms.br/~mzanusso/Data_Mining.htm>. Acesso em: 7 jul. 2015.

BRASIL. *Anteprojeto de Proteção de Dados Pessoais.* Disponível em: <http://participacao.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/>. Acesso em: 20 mar. 2015.

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil*. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 7 jul. 2015.

_____. *Projeto de Lei do Senado n. 181 de 2014.* Disponível em<http://www2.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=B68F55E7C7EA3C5F2DCB830D8767A41A.proposicoesWeb2?codteor=1001750&filename=PL+4060/2012>. Acesso em: 3 mar. 2015.

CANOTILHO, José Joaquim Gomes. *Estudos sobre direitos fundamentais*. São Paulo: Revista dos Tribunais; Portugal: Coimbra, 2008.

CONJUR. *Marco civil da internet e proteção de dados pessoais vão a debate***.**<Disponível em: http://www.conjur.com.br/2015-jan-27/marco-civil-internet-protecao-dados-pessoais-debate>. Acesso em: 27 jun. 2015.

_____. *STJ decidem se consumidores podem pedir dados em sistema de avaliação de risco.* Disponível em: <http://www.conjur.com.br/2015-fev-26/stj-decide-consumidores-podem-pedir-exibicao-dados-scoring> . Acesso em: 15 mar. 2015.

DIRETIVA 95/46/CE. *DIRECTIVA 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995.* Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:pt:HTML>. Acesso em: 20 mar. 2015.

DONEDA, Danilo (org). *A proteção de dados pessoais nas relações de consumo*: para além da informação creditícia. Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010.

FERRAZ Jr., Tercio Sampaio. *Direito constitucional:* liberdade de fumar, privacidade, Estado, Direitos Humanos e outros temas. Barueri, SP: Manole, 2007.

_____. *Sigilo bancário.* Disponível em: <http://www.terciosampaioferrazjr.com.

br/?q=/publicacoes-cientificas/98>. Acesso em: 4 maio 2015.

FERREIRA Filho, Alberto; GOMES, Andreia de Andrade. *Privacidade versus poder no anteprojeto de proteção de dados pessoais.* Disponível em: <http://www.conjur.com.br/2015-fev-20/privacidade-versus-poder-projeto-protecao-dados-pessoais>. Acesso em: 20 mar. 2015.

GONÇALVES, Maria Eduarda. *Direitos de informação.* Almedina: Coimbra, 1994.

KHOURI. Paulo R. Roque. A. *Direito do consumidor*: contratos, responsabilidade civil e defesa do consumidor em juízo. São Paulo: Atlas, 2013.

LOBO, Ana Paula. *Brasileiros não confiam nas empresas e descartam proteção a dados pessoais*. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=39460&sid=97#.VYSzAflViko>. Acesso em: 20 jun. 2015.

LUARO, Regina Linden; RODRIGUES, Daniel Piñero; FINGER, Brunize (col). O direito à proteção de dados pessoais e a privacidade. Curitiba: *Revista da Faculdade de Direito* – UFP. n. 53, 2011.

MENDES, Gilmar Fereira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. *Curso de direito constitucional*. São Paulo: Saraiva, 2010.

_____. Colisão de direitos fundamentais: liberdade de expressão e de comunicação e direito à honra e à imagem. *Revista Informação Legislativa*, n. 31, maio/jun., 1994. Disponível em: <file:///C:/Users/Usuario/Downloads/colisao%20de%20direitos%20fundamentais%20liberdade%20de%20expressao%20e%20de%20comunicacao%20e%20direito%20a%20honra%20e%20a%20imagem.pdf>. Acesso em: 15 jun. 2015.

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

NOVAES, Rafael. *Quais são os riscos dos tracking cookies?* Disponível em: <http://www.psafe.com/blog/tracking-cookies-quais-sao-riscos/>. Acesso em: 7 jul. 2015.

TI INSIDE ONLINE. *União Europeia discute lei que endurece regras sobre privacidade de dados*. Disponível em: <http://convergecom.com.br/tiinside/10/03/2015/uniao-europeia-discute-lei-que-endurece-regras-sobre-privacidade-de-dados/#.VZ68VSJShBs> . Acesso em: 20 maio 2015.

UOL SEGURANÇA ONLINE. *O que são cookies e como eles podem me prejudicar?* Disponível em: <http://seguranca.uol.com.br/antivirus/dicas/curiosidades/o-que-sao-cookies-e-como-eles-podem-me-prejudicar.html#rmcl>. Acesso em: 7 jul. 2015.

VAZQUEZ, 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. XXI Congresso Nacional do CONPEDI/UFF, outubro de 2012.

WARREN, Samuel; BRANDEIS, Louis D. The right to privacy. *Havard Law Review*, v.4, p.193, dec. 1890. Disponível em: <http://www.estig.ipbeja.pt/~ac_direito/privacy.pdf>. Acesso em: 10 jun. 2015.

Artigo recebido em 16/05/2016
Artigo aprovado em 15/06/2016