A NECESSIDADE DE UM CÓDIGO BRASILEIRO DE PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

Matheus Nunes Tajra[1]

Joana de Moraes Souza Machado[2]

Sumário: Introdução. 1 A expansão do conceito de privacidade. 2 O modelo italiano de proteção de dados pessoais. 3 A proteção de dados pessoais no Brasil. 4 A responsabilidade civil das empresas de tratamento de dados pessoais. Conclusão. Referências.

RESUMO

Com a evolução tecnológica, a criação e expansão dos bancos de dados, sobreveio o aumento dos abusos no âmbito do tratamento de informações pessoais. Com frequência, é possível identificar violações dos princípios de tratamento, em casos de utilização ilícita ou inexata dos dados pessoais, para finalidades distintas da que motivou a sua coleta, conservação sem a observância das normas de segurança, dentre outros. Tratam-se de situações que, de algum modo, geram dano aos titulares das informações e, portanto, devem ensejar a responsabilidade civil dos responsáveis. Diante da falta de legislação específica no Brasil regulando a matéria, julga-se relevante a análise do modelo europeu de proteção de dados pessoais, tomando a legislação italiana como inspiração. Vale ressaltar que um passo decisivo para suprir essa lacuna foi dado com a apresentação de um Anteprojeto de Lei de Proteção de Dados Pessoais.

Palavras-chave: Direito à privacidade; tratamento de dados pessoais; bancos de dados; responsabilidade civil.

ABSTRACT

With the technological evolution, the databases' creation and expansion, came the increase in abuse in the processing of personal information. It is often possible to identify violations of the treatment's principles in cases of misuse or inaccurate personal data, for different purposes of which led to its collection, conservation without compliance with the safety standards, among others. These are situations that somehow generate damage to the holders of information and, therefore, should give rise to civil liability of those responsible. Given the lack of specific legislation in Brazil governing the subject, it is deemed relevant the analysis of the European model of personal data protection, taking the Italian legislation as inspiration. It is noteworthy that a decisive step towards filling this gap was taken with the presentation of a Draft Personal Data Protection Act.

Keywords: Right to privacy; personal data processing; databases; civil responsability.

[1] Graduando em Direito pela Universidade Federal do Piauí – UFPI. Bolsista do Programa Institucional de Bolsas de Iniciação Científica - PIBIC/UFPI.

[2] Coordenadora do Curso de Direito do Centro Universitário Uninovafapi, Professora Adjunta da Universidade Federal do Piauí – UFPI, Doutora em Direito Constitucional pela Universidade de Fortaleza – UNIFOR, Mestre em Direito e Desenvolvimento pela Universidade Federal do Ceará – UFC.

INTRODUÇÃO

Apesar de todos os benefícios e comodidades decorrentes do desenvolvimento tecnológico das últimas décadas, tem-se assistido ao aumento exponencial da utilização de informações pessoais, de grande valia para determinados nichos do mercado, especialmente os setores de crédito e de consumo de bens e serviços. Na mesma velocidade, verificou-se o aumento dos casos de abuso nessa seara, notadamente no que se refere ao tratamento de dados pessoais, ou seja, qualquer atividade que envolva esse tipo de informações, tais como a sua coleta, manipulação e armazenamento em bancos de dados.

Diante dessa realidade, urge aprofundar os estudos sobre a privacidade na sociedade da informação. Para tanto, cabe tentar delimitar as esferas de intimidade, vida privada e vida pública, termos muitas vezes utilizados indistintamente pela doutrina, e confundidos com a própria ideia de privacidade. Essa dificuldade de estabelecer um conceito melhor delimitado para a privacidade se justifica pelo fato de o seu desenvolvimento depender diretamente das particularidades de cada sociedade. Por isso, entende-se necessário apresentar as suas diversas fases ao longo da história, desde a antiguidade, avançando pela idade média, até sua concepção contemporânea, moldada pela noção de autodeterminação informativa.

No que tange aos instrumentos de tutela da privacidade, surgiram dois modelos preponderantes no mundo jurídico, o norte-americano e o europeu. É inegável que ambos têm suas virtudes, mas o modelo europeu parece mais adequado para uma efetiva tutela da privacidade, sob a égide das Diretivas 95/46/CE e 2002/58/CE da União Europeia, que tem como cerne a proteção da dignidade e dos direitos fundamentais da pessoa humana. Nesse sentido, merece destaque a legislação em matéria de proteção de dados da Itália, que passou por um esforço de uniformização no início dos anos 2000, com o advento do Decreto Legislativo 196/2003.

No Brasil, inexiste legislação específica sobre proteção de dados pessoais, o que representa uma ameaça ao direito à privacidade dos indivíduos, expostos a condutas ilícitas e abusivas dos agentes responsáveis pelo tratamento de dados. Apesar de a aprovação do Marco Civil da Internet ter representado um avanço para a regulação de atividades relacionadas ao meio cibernético, essa lei não disciplinou de forma detalhada a proteção de dados pessoais. Da mesma forma, verifica-se a insuficiência do instituto do *habeas data* e do Código de Defesa do Consumidor para a tutela da privacidade.

Dessa forma, faz-se necessária, com urgência, a aprovação de legislação específica sobre a matéria. Uma via interessante parece ser o Anteprojeto de Lei de Proteção de Dados Pessoais, apresentado pelo Ministério da Justiça, que visa a estabelecer requisitos para o tratamento de dados pessoais, que deve ser regido por uma série de princípios, nos moldes do Código Italiano em Matéria de Proteção de Dados Pessoais.

1 A EXPANSÃO DO CONCEITO DE PRIVACIDADE

A doutrina brasileira utiliza para se referir à privacidade, muitas vezes indistintamente, termos como vida privada, intimidade, segredo, sigilo e recato. Fenômeno similar se repete em outros países, tendo em vista a impossibilidade de delimitar um conceito rígido e universal para a privacidade, cujo desenvolvimento está diretamente relacionado às particularidades de cada sociedade e, portanto, de acordo com os respectivos ordenamentos jurídicos.

De acordo com Danilo Doneda (2006), o vocábulo "privacidade" tem raiz latina (o verbo *privare*, cuja forma adjetiva é *privatus*), muito embora hoje seja utilizado principalmente em razão do seu intenso emprego na língua inglesa. Ao discorrer sobre os termos intimidade e vida privada, o autor cita a doutrina de Hubmann, segundo a qual os diferentes graus de manifestação do sentimento de privacidade são representados por um esquema de círculos concêntricos. O círculo mais interno corresponderia à esfera da intimidade ou do segredo, seguido pela vida privada, de maior diâmetro, sem esquecer de outra ainda mais abrangente – a esfera pessoal, que inclui a vida pública do indivíduo.

Autores como Paulo José da Costa Júnior (1995), por sua vez, defendem que existiriam pelo menos três esferas da privacidade: vida privada, intimidade e segredo. A vida privada, esfera de maior diâmetro, consistiria nos fatos e comportamentos que a pessoa não quer que se tornem públicos. A intimidade, um pouco mais reduzida, seria aquela em que participam pessoas nas quais o indivíduo deposita certa confiança. O segredo, esfera mais interna, corresponderia a um espaço em que as informações não são compartilhadas ou, no máximo, o são com um número restrito de pessoas, bastante próximas do indivíduo.

Em contraponto às referidas esferas da privacidade, existe a vida pública, que diz respeito a informações de natureza pública sobre o indivíduo, de conhecimento de uma coletividade indeterminada de pessoas. Vale ressaltar que, segundo o autor, a linha que define cada uma dessas esferas é tênue, variando de acordo com a condição socioeconômica ou a natureza da profissão do sujeito.

A Constituição Federal de 1988 consagrou expressamente a proteção da "intimidade" e da "vida privada" em seu artigo 5º, inciso X. Nesse contexto, entende-se a intimidade como uma esfera da privacidade ainda mais íntima do que a vida privada. Trata-se de um espaço impenetrável e indevassável, que diz respeito apenas ao próprio indivíduo, como recordações pessoais, memórias, diários etc. A esfera da intimidade abrange também, portanto, a do segredo, ou seja, os assuntos delicados a ponto de a pessoa não desejar partilhar com ninguém. A vida privada, por outro lado, é relativa a um espectro mais amplo, que inclui questões sobre a família da pessoa, saúde física e mental, dentre outros. Consiste em uma esfera que, a princípio, veda a intromissão de outrem, mas que pode ser partilhada, de acordo com o desejo e a conveniência do indivíduo.

Destarte, percebe-se que o constituinte fez uso de ambos os termos com o objetivo de assegurar a máxima aplicabilidade da norma, uma vez que se tratam de expressões com significados distintos. A esse respeito, Sidney Guerra aduz que:

> De toda sorte, o constituinte preocupou-se em assegurar a inviolabilidade da intimidade e da vida privada – o primeiro rejeita qualquer espécie de interferência, quer pública quer privada, enquanto que o segundo rechaça a interferência do conhecimento público – pelo fato de tais direitos estarem sendo ameaçados, com bastante frequência, por investigações e divulgações ilegítimas, realizadas por aparelhos registradores de imagem, sons e dados, infinitamente sensíveis aos olhos e ouvidos (GUERRA, 2004, p. 55).

O termo privacidade, de maior amplitude no direito brasileiro, parece ser o mais adequado para expressar o sentido de vida privada e intimidade e, por isso, foi o adotado nesta obra. Na mesma direção inclina-se a maior parte da doutrina, que considera que a despeito das questões terminológicas, a ideia de privacidade é capaz de melhor expressar o objetivo comum da matéria: a tutela da pessoa humana diante da complexidade de situações subjetivas.

Para uma melhor compreensão do tema, é pertinente apresentar as diferentes fases da ideia de privacidade ao longo da história. Doneda (2006) cita algumas situações relacionadas à privacidade, encontradas na filosofia antiga, com base na obra de Sêneca, segundo o qual a amizade e a fidelidade estariam entre os mais altos sentimentos humanos, sendo alcançados somente através da intimidade e do retiro.

Em Roma antiga também era possível constatar o respeito à privacidade e ao segredo, especialmente nas práticas religiosas e festividades familiares. Cícero, por exemplo, repudiava a divulgação de segredos de pessoas privadas. Entretanto, é preciso ressaltar que não se pode atribuir à privacidade valorizada pelos romanos a concepção atual de individualismo, devendo antes ser entendida como um refúgio dos negócios da *res publica*. Assim, não se pode afirmar

que a privacidade já se apresentava como direito individual, tendo em vista que o homem participava da vida coletiva basicamente como parte de seu grupo (DONEDA, 2006).

Na Idade Média, apenas uma parcela privilegiada da população tinha condições de manter certo isolamento em relação aos demais, como alguns senhores feudais, além de religiosos e místicos que optaram pela solidão. Com o tempo, os senhores feudais mais influentes teriam começado a ansiar por uma esfera privada em moldes similares aos atuais, o que se manifestava através do desejo de intimidade no pensamento, intimidade durante o sono, durante as refeições, nos rituais religiosos e sociais (DONEDA, 2006).

Diante do esfacelamento da sociedade feudal e da ascensão da classe burguesa, constata-se o nascimento da privacidade na sua concepção moderna, como consequência do individualismo burguês. O advento de um novo modelo de construção das cidades e habitações e a separação entre o local de residência e o de trabalho, por exemplo, foram fatores que contribuíram de forma decisiva para a conquista da privacidade pela burguesia. Dessa forma, como defende Stefano Rodotà (2008), pode-se afirmar que o nascimento da privacidade não se apresenta como a realização de uma exigência natural de cada indivíduo, mas como a aquisição de um privilégio por parte de um grupo.

Na realidade, a privacidade guardava maior proximidade com a ideia de propriedade do que com a liberdade ou a autonomia dos indivíduos. Prova disso é sua tendência ao desaparecimento na medida em que se tornam menos abastados os indivíduos, como ocorria com a pequena burguesia europeia confinada em habitações populares na periferia das grandes cidades. Como adverte Rodotà (2008), foram as condições materiais de vida que excluíram a privacidade dos horizontes da classe operária.

Assim, percebe-se que no século XIX a ideia de privacidade estava profundamente atrelada à possibilidade material de assegurá-la, sendo o direito de propriedade entendido como condição imprescindível para a sua conquista. Por essa razão, a classe operária somente teve seu direito à privacidade reconhecido bem mais tarde, através de instrumentos jurídicos distintos, como a tutela da personalidade nas fábricas.

Nessa toada, a tutela da privacidade nos países de common law esteve atrelada desde o início às regras de proteção da propriedade privada. No ordenamento jurídico brasileiro, desde a Constituição de 1824 há previsão expressa da inviolabilidade do domicílio e da correspondência, matizes do direito à privacidade.

Em 1890, os advogados Louis Brandeis e Samuel Warren publicaram na Harvard Law Review o artigo "The right to privacy"[3], considerado por muitos o marco do início do debate moderno sobre a privacidade. Brandeis e Warren defendiam uma fundamentação diversa para a proteção da privacidade[4], que teria como princípio basilar a tutela da personalidade, não a propriedade privada. Doneda (2006) aponta que o referido artigo propôs uma força inédita ao novo direito à privacidade, atribuindo a sua influência a algumas de suas características:

> (i) partia-se de um novo fato social, que eram as as mudanças trazidas para a sociedade pelas tecnologias de informação (jornais, fotografias) e a comunicação de massa; (ii) o novo "direito à privacidade" era de natureza pessoal, e não se aproveitava da estrutura da tutela da propriedade para proteger aspectos da privacidade; (iii) no que interessa somente aos EUA, o artigo abriu o caminho para o reconhecimento (que porém ainda tardaria décadas) do direito à privacidade como um direito constitucionalmente garantido (DONEDA, 2006, p. 139).

Em face do desenvolvimento tecnológico e o crescimento dos bancos de dados, as discussões sobre privacidade passaram a versar principalmente acerca da necessidade de que sejam assegurados ao indivíduo meios de exercer o controle dos poderes baseados na disponibilização de informações a seu respeito, armazenadas e utilizadas por terceiros. A esse respeito, preleciona Rodotà (2008, p. 245) que a tutela dos dados pessoais não diz respeito somente à divulgação imprópria das informações de determinado indivíduo, mas consiste também na defesa da esfera privada contra invasões que violem o seu direito à tranquilidade e eliminem o direito de não saber.

2 O MODELO ITALIANO DE PROTEÇÃO DE DADOS PESSOAIS

Diante do brutal desenvolvimento tecnológico das últimas décadas, fazia-se necessário que os mais diversos ordenamentos jurídicos formulassem mecanismos eficientes de tutela da privacidade, de forma a assegurar a proteção de dados pessoais. Nesse contexto, se consolidaram dois modelos de disciplina da matéria: o norte-americano e o europeu.

O primeiro, de caráter fragmentado, é marcado pelas disposições legislativas e jurisprudenciais concorrentes, com a proteção das informações pessoais assegurada em legislação esparsa, federal e estadual. O caráter constitucional do direito à privacidade

[3] Warren, à época da publicação do artigo, era sócio de Brandeis na advocacia privada e casado com a filha de Thomas F. Bayard, influente senador. As divulgações pela imprensa local de detalhes da suntuosa comemoração de seu casamento, além da presença constante de sua família nos noticiários da época, teriam despertado o seu inconformismo com a intrusão de terceiros na vida privada do cidadão. Brandeis, que posteriormente se tornou um dos juízes de maior prestígio da Suprema Corte dos Estados Unidos, por sua vez, debruçou-se sobre o tema influenciado pelos filósofos transcendentalistas Emerson e Thoureau, tendo proferido diversas decisões envolvendo a privacidade.

[4] O artigo tratava especificamente do direito à privacidade no que concerne à publicação de escritos pessoais.

somente foi reconhecido nos Estados Unidos em razão da grande influência de algumas decisões proferidas pela Suprema Corte e por outros tribunais, uma vez que a constituição norte-americana, de 1787, não trata expressamente da matéria. (DONEDA, 2006)

Já o modelo europeu, sistemático, estrutura-se em torno da Diretiva 95/46/CE da União Europeia, uma disciplina ampla e detalhada que é transposta para a legislação interna de cada Estado-membro. Vale ressaltar que este foi fortemente influenciado pela Convenção de Strasbourg, segundo a qual a proteção de dados pessoais estaria diretamente relacionada à proteção dos direitos humanos e das liberdades individuais, figurando como pressuposto do estado de direito. (DONEDA, 2006)

Por seu elevado grau de sistematização e universalidade, o modelo europeu parece mais adequado para uma efetiva tutela da privacidade, apta a garantir um nível mínimo de proteção. A despeito de a diretiva ter estabelecido parâmetros comuns a serem seguidos pelos países do bloco, é pertinente lembrar a cada nação foi atribuída a competência para editar lei própria que incorporasse as normas comunitárias, de forma a garantir a integração com o seu ordenamento.

Dessa maneira, optou-se neste trabalho pela abordagem da legislação em matéria de proteção de dados da Itália, e não pela análise do modelo europeu "genérico". Tal escolha pode ser justificada em razão do considerável desenvolvimento do ordenamento italiano nessa seara nas últimas décadas. No decorrer de mais de vinte anos, diversos projetos de lei foram elaborados e descartados, com grande influência da doutrina. Somente em dezembro de 1996 a Itália aprovou a lei 675/96, que efetivou a incorporação do conteúdo da Diretiva 95/46/CE para o direito interno italiano – penúltimo país da União Europeia a elaborar uma lei de proteção de dados pessoais, se valeu da experiência dos outros países sobre o tema.

Outro aspecto notável da legislação italiana supracitada é o fato de ter sido inteiramente elaborada de acordo com a Diretiva, ao contrário de diversos países do bloco europeu que já tinham leis próprias sobre a matéria e precisaram reformular os pontos que contrariavam a nova diretriz. Destarte, a lei italiana reflete o padrão de tratamento adotado pela União Europeia para regular a matéria, "com características próprias como seu acentuado caráter de instrumento de tutela da pessoa, ao contrário das leis de outros países que acentuaram a ligação da disciplina da informação com a tecnologia". (DONEDA, 2006, p. 255)

No que tange efetivamente ao seu conteúdo, a lei 675/96 estabeleceu na Itália um sistema de proteção de dados com base na delimitação de um sistema de autorizações e responsabilidades para as empresas de tratamento de dados pessoais, fixou os direitos do interessado e consagrou princípios aplicáveis à matéria. Além disso, criou a Autoridade Garante, um organismo com a atribuição de zelar pela proteção dos dados pessoais.

Doneda (2003) destaca a aprovação, no mesmo dia da legislação em comento, a lei 675/96, que delega ao executivo a faculdade de legislar sobre parâmetros para a posterior integração e correção da lei 675/96. Nessa esteira, se seguiram diversas alterações no ordenamento italiano em matéria de proteção de dados, por meio de uma série de Decretos Presidenciais e Legislativos.

Como ápice da evolução dessa integração normativa pode-se apontar o Decreto Legislativo 196/2003, também denominado Código em Matéria de Proteção de Dados Pessoais. O referido código incorporou a lei 675/96, bem como toda a legislação suplementar sobre o tema e a Diretiva 2002/58/CE sobre a proteção de dados pessoais nas comunicações eletrônicas. Assim, percebe-se que o código reflete um esforço na direção de racionalizar e sistematizar a legislação anterior sobre a matéria, ao reunir normas específicas de tratamento de dados para vários setores. Sobre a organização do Decreto Legislativo, Danilo Doneda aduz:

> O código é estruturado em três partes. A primeira, geral, é denominada "disposições gerais" e estabelece a normativa substancial a ser aplicada a todas as modalidades de tratamentos de dados pessoais, com o núcleo essencial dos princípios atinentes à matéria. A segunda, algo como uma parte "especial", denomina-se "disposições relativas a setores específicos" e congrega normas específicas a determinados setores (como os dados judiciários, sanitários ou informações sobre credores e trabalhadores, por exemplo). Na terceira, de nome "tutela do interessado e sanções", encontram-se disposições sobre o sistema e os instrumentos de tutela adotados, administrativos e judiciários, e sobre as formas de tutela. (DONEDA, 2006, p. 257)

Um dos aspectos mais marcantes do Código Italiano em Matéria de Proteção de Dados Pessoais é a sua natureza principiológica, que reflete a preocupação do legislador de garantir a coerência global da disciplina, extremamente dinâmica. Danilo Doneda (2003), entende que essa opção por uma legislação por princípios tem como grande vantagem a facilidade de adaptação de seus dispositivos diante das constantes mudanças ditadas pelo desenvolvimento tecnológico.

Assim, o sistema italiano de proteção de dados pessoais estrutura-se com base em uma série de princípios que regem a atividade de tratamento de dados, como o princípio da

finalidade e da necessidade, consagrados no artigo 11 do Decreto Legislativo 196/2003[5]. Esses princípios assumem especial importância na medida em que são utilizados como instrumento de defesa do direito à privacidade – na forma de direito fundamental à proteção de dados pessoais. Através da sua aplicação, pretende-se garantir aos indivíduos o efetivo exercício da autodeterminação informativa, isto é, o controle da circulação dos seus dados na sociedade, através dos direitos de acesso, cancelamento e retificação de dados[6].

Percebe-se, portanto, a preponderância dos princípios para a proteção dos dados pessoais: ao estabelecer limites para o seu tratamento e fluxo, balizam a atividade, visando a evitar excessos por parte das empresas responsáveis. Cabe apresentar uma síntese dos princípios mais relevantes pertinentes à matéria, elaborada por Doneda (2009), levando em consideração o conteúdo comum das leis e diretivas sistematizadas no *códex* em comento:

> - Princípio da Finalidade: estipula que os dados somente poderão ser coletados e tratados para o cumprimento das finalidades legítimas, previamente determinadas e comunicadas no momento da coleta e relacionadas com a atividade de quem os trate;
> - Princípio do Tratamento leal e lícito: estipula que os dados devem ser coletados e tratados de boa-fé, na observância da lei. Não podem ser tratados de forma diversa daquela que motivou a sua obtenção, a não ser com a autorização expressa do seu titular;
> - Princípio da Proporcionalidade: estipula que somente poderão ser tratados os dados que forem adequados, pertinentes e não excessivos em relação às finalidades que motivaram a sua coleta;
> - Princípio da Exatidão: estipula que os dados devem se manter exatos, completos e atualizados, fazendo referência à verdadeira situação da pessoa a qual se referem;
> - Princípio da Conservação: estipula que os dados devem ser cancelados ou tornados anônimos quando deixam de ser necessários para o cumprimento das finalidades que justificaram sua coleta e tratamento;
> - Princípio da Segurança Física e Lógica: estipula que os dados devem ser protegidos contra os riscos de seu extravio, destruição, perda, transmissão ou acesso não autorizado;
> - Princípio do Livre Acesso: estipula que o titular dos dados deve ter acesso irrestrito aos seus dados armazenados por terceiros, podendo obter cópias de seus registros e solicitar a sua correção, se necessário;

[5] O título III do código estabelece as regras gerais para todos os tratamentos de dados. Dispõe o art. 11: "Modalidade do tratamento e requisitos dos dados. 1. Os dados pessoais objeto de tratamento são: a) tratados de modo lícito e com correção; b) colhidos e registrados para finalidades específicas, explícitas e legítimas, e utilizados em outras operações de tratamento segundo formas compatíveis com tais escopos; c) exatos e, se necessário, atualizados; d) pertinentes, completos e não excessivos em relação às finalidades para as quais são colhidos ou posteriormente tratados; e) conservados de forma a permitir a identificação do interessado por um período de tempo não superior ao necessário aos escopos para os quais foram colhidos ou posteriormente tratados. 2. Os dados pessoais tratados com violação da disciplina referente ao tratamento de dados pessoais não podem ser utilizados".

[6] O art. 7º do código determina: "Direito de acesso aos dados pessoais e outros direitos. 1. O interessado tem direito a obter a confirmação da existência ou não de dados pessoais que lhe digam respeito, mesmo se ainda não registrados, e de obter uma cópia destes em uma forma inteligível. 2. O interessado tem direito de obter a indicação: a) da origem dos dados pessoais; b) das finalidades e das modalidades de tratamento; (...) 3. O interessado *tem direito de obte*r: a) *a atualização, a retificação ou*, quando houver interesse, a *integração dos dados*; b) *a eliminação, a transformação em forma anônima ou o bloqueio dos dados tratados com violação da lei*, incluídos aqueles cuja conservação não é necessária para as finalidades para as quais foram colhidos ou posteriormente tratados" (...).

> - Princípio da Necessidade: estipula que os dados pessoais somente serão objeto de tratamento quando a finalidade almejada não puder ser atingida de outra maneira. (DONEDA, 2009, p. 686-687)

Em contrapartida, há quem se preocupe com uma possível falta de efetividade da tutela da privacidade, sob a alegação de que a resposta do código às inovações tecnológicas seria excessivamente lenta apesar da flexibilidade própria das legislações por princípios. A própria Diretiva 95/46/CE apresenta uma resposta satisfatória para essas críticas: a manutenção da utilização dos princípios combinada com a criação de instrumentos que garantam maior eficácia concreta e coercibilidade. (DONEDA, 2003)

Para assegurar que o tratamento de dados pessoais seja empreendido segundo os ditames legais e obedecendo os princípios que regem a matéria, o Código Italiano em Matéria de Proteção de Dados Pessoais previu em seu art. 153 a figura de uma Autoridade Garante. Trata-se de um órgão colegiado[7], independente da estrutura da administração pública, cujas atribuições incluem, dentre outras: verificar se os tratamentos são realizados no respeito da disciplina aplicável (art. 154.1.a), prescrever aos titulares do tratamento as medidas necessárias ou oportunas para tornar o tratamento conforme as disposições vigentes (art. 154.1.c) e vetar, mesmo que ex officio, total ou parcialmente, o tratamento ilícito ou incorreto dos dados ou bloqueá-los (art. 154.1.d). Doneda (2006) defende que a atuação do referido órgão merece detida consideração:

> Em primeiro lugar, porque neste caso a mera atuação do indivíduo para a proteção de seus interesses – o controle individual, como ocorre em algumas das concepções de proteção de dados pessoais que nós verificamos [o modelo norte-americano] – não é capaz de projetar uma situação na qual o direito fundamental em questão receba tutela adequada e acaba por espelhar uma determinada concepção ideológica dos interesses em questão que, amenizada por uma aparente concessão de poder ao indivíduo, não acarreta na tutela efetiva de seus interesses. A impossibilidade de uma autodeterminação informativa baseada na ação singular de seu interessado é patente em vista da desproporção entre sua vontade e a existência de estruturas destinadas à coleta de seus dados e preparadas a excluí-lo de certas vantagens caso decida por não fornecê-los (DONEDA, 2006, p. 399)

Ademais, ao Garante é atribuída a função de promover a confirmação dos códigos deontológicos[8] das várias categorias profissionais que atuam na atividade de tratamento de

[7] Dispõe o art. 153.2 do código: "o Garante é um órgão colegiado, constituído por quatro componentes, dois deles eleitos pela Câmara dos Deputados e dois pelo Senado da República com voto limitado. Os componentes são escolhidos entre pessoas que assegurem independência e que sejam especialistas de notória competência nas matérias do direito ou da informática, garantindo a presença de ambas as qualificações".

[8] O art. 12 do código prevê a participação do Garante na elaboração de códigos deontológicos e de boa conduta: "1. O Garante promove no âmbito das categorias interessadas, observando-se o princípio da representatividade e levando-se em conta os critérios diretivos das recomendações do Conselho da Europa sobre tratamento de dados pessoais, a subscrição de códigos deontológicos e de boa conduta para determinados setores, verifica sua conformidade às leis e aos regulamentos também pelo exame de observações dos sujeitos interessados e contribui para garantir sua divulgação e o respeito aos mesmos".

dados pessoais. A opção por facultar a cada setor a elaboração de seu próprio código de boas condutas decorre da existência de necessidades específicas, que exigem a regulação de aspectos práticos de cada atividade.

Assim, se pretende fazer com que os princípios gerais em matéria de proteção de dados pessoais conquistem um maior grau de aproximação da realidade e, portanto, alcancem maior efetividade. Destaque-se que, por se tratar de matéria em constante diálogo com a técnica, e na qual certezas e dogmas chegam com demasiada facilidade à obsolescência, são imprescindíveis instrumentos adaptáveis a novas situações, capazes de garantir uma tutela forte no caso concreto (DONEDA, 2009). O sistema jurídico italiano busca essa tutela satisfatória justamente por meio da complementaridade entre o código, as normas setoriais e a regulação administrativa, esta última a cargo do Garante.

3 A PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

A tutela da privacidade no ordenamento jurídico brasileiro é tema tratado em sede constitucional, tendo sido incluídos no rol de direitos fundamentais da Constituição Federal de 1988 a proteção da intimidade, da vida privada, a honra e a imagem dos indivíduos, na forma do art. 5º, inciso X. Ademais, o inciso XII do mesmo artigo garante a inviolabilidade do sigilo de dados, enquanto o inciso LXXII prevê o remédio constitucional do *Habeas Data*, para citar apenas alguns dos dispositivos mais significativos para a disciplina da proteção de dados pessoais.

O *habeas data*, uma inovação da CF/1988, consiste em um instrumento que visa a resguardar o direito à privacidade do indivíduo, na medida em que possibilita que postule em juízo o conhecimento e a retificação de informações constantes de registros ou bancos de dados de caráter público. A lei 9.507/97, por sua vez, regulamentou os direitos garantidos no inciso LVII do art. 5º da CF[9] e disciplinou o procedimento judicial do habeas data. A respeito do caráter do instituto e do contexto histórico de sua criação, aduz Danilo Doneda:

> O habeas data é um instituto de caráter remedial, como o *writ of mandamus* (EUA) ou o *amparo* (Espanha, México e outros países). No direito brasileiro, é uma das ações constitucionais que formam um rol de instrumentos para a garantia de direitos individuais e coletivos. Esta sua posição no ordenamento deve ser entendida no âmbito de um movimento de reação, que se deu no momento em que a sociedade e o próprio ordenamento se recompunham de um período no qual diversas liberdades individuais foram suprimidas. Neste contexto, o *habeas data* foi uma das medidas

[9] Dispõe o art. 5º, inciso LXXII da CF/1988: "conceder-se-á habeas data: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo".

> destinadas a sanar um "déficit" de liberdades individuais, bem como consolidar as bases democráticas do novo sistema. (DONEDA, 2006, p. 332-333)

A despeito da louvável iniciativa do constituinte ao introduzir o instituto no sistema jurídico, a ponto de influenciar outras legislações latino-americanas, constata-se na prática que o *habeas data* tem eficácia duvidosa quanto a assegurar a proteção do direito material a que se propõe. Primeiro, pelo fato de o remédio constitucional em comento somente ser previsto para as hipóteses de bancos de dados de entidades governamentais ou de caráter público, excluídos, portanto, a contrário sensu, os bancos de dados privados. Ademais, a necessidade de tentativa prévia de obtenção dos dados por via administrativa, nos termos do art. 8º, parágrafo único[10] da lei 9.507/97, limita consideravelmente a possibilidade de manejo do *writ*.

Dessa forma, persiste a prática de abusos na atividade de tratamento de dados pessoais, apesar da relevância do *habeas data* como instrumento processual de defesa da privacidade. Cabe ressaltar que este não permite que o titular dos dados exerça qualquer controle sobre a manipulação e o tratamento das informações que as empresas públicas ou privadas detenham a seu respeito, tendo em vista que somente é aplicável quando o indivíduo deseja obter ou retificar informações a seu respeito (MACHADO, 2015).

No âmbito da legislação infraconstitucional, avanços significativos foram conquistados com o advento da lei 8.078/90, o Código de Defesa do Consumidor, que inclui uma seção que trata dos bancos de dados e cadastros de consumidores. Com o intuito de buscar o equilíbrio das relações de consumo, os artigos 43 e 44 do CDC impõem limites ao uso de informações pessoais dos consumidores pelos fornecedores. Leandro Lages (2015) esclarece que a legislação consumerista permite a criação de cadastros de inadimplentes, com a possibilidade de compartilhamento de informações pelos fornecedores, porém assegura aos consumidores o livre acesso a esses dados, assim como o direito a certidão escrita no que tange a eles.

Outras limitações são previstas no artigo 43 do CDC, que dispõe que o registro de dados negativos sobre um consumidor não pode ser mantido por período superior a cinco anos, havendo necessidade de comunicação escrita sobre o tratamento de dados pessoais e de

[10] O art. 8º, parágrafo único da lei 9.507/97 estabelece que: "a petição inicial deverá ser instruída com prova: I - da recusa ao acesso às informações ou do decurso de mais de dez dias sem decisão; II - da recusa em fazer-se a retificação ou do decurso de mais de quinze dias, sem decisão; ou III - da recusa em fazer-se a anotação a que se refere o § 2º do art. 4º ou do decurso de mais de quinze dias sem decisão".

consumo, quando não solicitadas pelo consumidor. Além disso, Doneda (2006) cita o direito de acesso, correção e, implicitamente, o cancelamento justificado dos dados pessoais dos consumidores armazenados em bancos de dados.

Urge destacar a presença, neste diploma legislativo, de alguns dos princípios de proteção de dados pessoais, ainda que de forma simplificada e inseridos no contexto das relações de consumo, o que impediria a sua utilização como sistema geral de proteção de dados pessoais. Um exemplo seria o princípio da finalidade, que pode ser reconhecido no ordenamento brasileiro por meio da aplicação da cláusula de boa-fé objetiva e da garantia constitucional da privacidade, podendo ser utilizado como fundamento para o reconhecimento da vedação da coleta de dados sensíveis[11] e da comercialização de bancos de dados de consumidores. (DONEDA, 2006)

Por outro lado, inexistia no Brasil legislação específica para o ambiente cibernético, incluindo a garantia à proteção de dados pessoais. Isso representava um risco ao direito fundamental à privacidade do cidadão, vulnerável a abusos no tratamento de informações que circulam no meio virtual a seu respeito. Indo além, consistia em um óbice à atuação satisfatória do poder judiciário, uma vez que a ausência de definição legal gerava decisões judiciais conflitantes, e mesmo contraditórias.

Nesse contexto, foi apresentado pelo poder executivo o projeto de lei 21.626/2011, que se tornou conhecido como o Marco Civil da Internet. Votado pelo Congresso Nacional e sancionado pela Presidente da República apenas em 2014, o Marco Civil – lei 12.965/2014 –, estabelece princípios, direitos e deveres para o uso da internet no país. Vale ressaltar que a sua estrutura se baseia em três pilares: a neutralidade, a privacidade e a liberdade de expressão.

No que tange ao segundo pilar, que interessa a este trabalho, a proteção da privacidade e dos dados pessoais são asseguradas no art. 3º do Marco Civil, elencadas entre os princípios que regem a disciplina do uso da internet. O art. 7º estabelece a inviolabilidade da intimidade e da vida privada, enquanto o seu art. 8° consolida o direito à privacidade e à liberdade de expressão nas comunicações como condição para o pleno exercício do direito de acesso à internet.

---

[11] Entende-se por dados sensíveis aqueles cuja utilização pode ensejar discriminação ou consequências especialmente lesivas, oferecendo riscos potenciais mais elevados do que a média para o seu titular e até mesmo para uma coletividade. Nesta categoria se podem citar aqueles relativos a raça, preferências políticas, religiosas e sexuais, histórico médico ou dados genéticos de um indivíduo.

Entretanto, a lei 12.965/2014 não disciplinou de forma detalhada a proteção de dados pessoais, papel que caberia a ulterior lei específica, nos termos do inciso III do art. 3º. De qualquer forma, deve-se registrar o avanço consignado no art. 7°, VIII da referida lei, segundo o qual precisam ser asseguradas aos usuários da internet informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de dados pessoais, que somente poderão ser utilizados para as finalidades pelas quais foram coletados. Além disso, conforme se depreende do disposto no inciso VII do art. 7º, o consentimento assume lugar de destaque em tal regulação, como reflexo da ideia de autodeterminação informativa, segundo a qual devem ser atribuídos ao titular meios de controle sobre as informações que lhe dizem respeito. (MACHADO, 2015)

O Marco Civil da Internet, portanto, representa um passo importante na direção da proteção do direito à privacidade no Brasil ao consolidar uma série de princípios aplicáveis ao uso da internet – e à proteção de dados, ainda que este não seja o seu foco. Machado (2015) observa que o diploma é aplicável a todas as situações em que esteja em perigo a privacidade do usuário, tendo antecipado algumas regras referentes ao tratamento de dados pessoais em razão da ausência de legislação específica sobre esta matéria.

O legislador optou por editar lei de natureza principiológica, com o intuito de privilegiar a sua capacidade de fazer frente às frenéticas mudanças do mundo da tecnologia. Não obstante a escolha tenha sido acertada, verifica-se a insuficiência do Marco Civil para regular o a matéria de proteção de dados pessoais, de imensa complexidade.

Ainda inexiste no ordenamento brasileiro legislação específica sobre o tratamento de dados pessoais, capaz de prever mecanismos efetivos de tutela, tais como previsão de autoridade competente para fiscalizar a atividade de tratamento ou de normas específicas que estabeleçam os deveres e responsabilidades das empresas do setor, com vistas a proteger a dignidade e os direitos fundamentais da pessoa, particularmente em relação à sua privacidade. Nessa toada, Machado (2015) preleciona:

> O fato é que o modelo brasileiro se revela genérico, insatisfatório e lacunoso. Necessita de urgente regulamentação por legislação específica para a proteção de dados pessoais, com previsão expressa de que toda informação só possa ser objeto de tratamento para atingir a finalidade para a qual foi disponibilizada. As informações só poderão ser transmitidas a terceiros, com o expresso consentimento do seu titular. Acrescente-se a estes requisitos, a imposição de sanções civil, penal e administrativa pelo descumprimento das regras de proteção de dados (MACHADO, 2015, p.48).

Diante dessa realidade, há mais de cinco anos o Ministério da Justiça, em colaboração com o Observatório Brasileiro de políticas Digitais do Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas, trabalha na elaboração de um anteprojeto de lei de proteção de dados pessoais. Entre novembro de 2010 e abril de 2011, o texto do referido anteprojeto de lei passou por debate público sobre a privacidade e a proteção de dados pessoais. (MACHADO, 2015)

Seguiram-se manifestações de juristas e setores da sociedade civil, que através de debates e relatórios, apresentaram críticas e sugeriram algumas alterações do texto original do anteprojeto. Em 2012, associações do setor de comunicação e marketing como ABEMD (Associação Brasileira de Marketing Direto), ABA (Associação Brasileira de Anunciantes) e ANER (Associação Nacional dos Editores de Revistas), participaram de reuniões com o Departamento de Proteção e Defesa do Consumidor do Ministério da Justiça e apresentaram uma proposta de Carta de Princípios[12] e de um Código de Autorregulamentação[13] para o Tratamento de Dados Pessoais.

Entende-se que essa participação da sociedade civil é primordial para que se garanta um texto final de lei capaz de proteger a pessoa em relação ao tratamento de seus dados pessoais, sem contudo comprometer as atividades de determinados setores da economia. Atentos a esta questão, o Ministério da Justiça lançou em janeiro de 2015 uma nova plataforma na internet para realizar consulta pública sobre a matéria, com o intuito de colher novas sugestões, cuja viabilidade seria analisada por técnicos e pelo governo.

Só então, em 20 de outubro de 2015 foi apresentada uma nova versão do Anteprojeto de Lei de Proteção de Dados Pessoais, elaborada pela Secretaria Nacional do Consumidor (Senacon) em conjunto com a Secretaria de Assuntos Legislativos do MJ. O anteprojeto, encaminhado à Casa Civil da Presidência da República, estabelece requisitos para o tratamento de dados pessoais, atividade que deve ser regida por uma série de princípios, nos moldes do Código Italiano em Matéria de Proteção de Dados Pessoais e sob influência das Diretivas da União Europeia, especialmente a Diretiva 95/46/CE.

O anteprojeto de lei visa a assegurar ao cidadão o controle e a titularidade sobre suas próprias informações, de forma a garantir o livre desenvolvimento de sua personalidade e

[12] Carta de Princípios para o Tratamento de Dados Pessoais (Minuta 01/12/2011). Disponível em: <http://www.abemd.org.br/interno/Carta_de_Principios.pdf>. Acesso em: 31 de mar. 2016.
[13] Código Brasileiro de Autorregulamentação para a Proteção aos Dados Pessoais (Minuta 01/12/2011). Disponível em: <http://www.abemd.org.br/interno/Codigo_Autorreg_DadosPessoaois.pdf>. Acesso em: 31 de mar. 2016.

dignidade. A fim de possibilitar maior clareza da legislação, o art. 5º lista alguns conceitos relevantes para a compreensão da disciplina, tais como: dado pessoal, tratamento, dados sensíveis, banco de dados, responsável, operador e encarregado.

Encerrando o capítulo das disposições preliminares do anteprojeto, o art. 6º enuncia os princípios que regem a atividade de tratamento de dados pessoais, à semelhança do art. 11 do Código Italiano. São eles: o princípio da finalidade, da adequação, da necessidade, do livre acesso, da qualidade dos dados, da transparência, da segurança, da prevenção e da não discriminação, devendo ser observada sempre a boa-fé.

Ao tratar dos requisitos para o tratamento de dados pessoais, o anteprojeto de lei teve o a preocupação de destacar a necessidade de consentimento livre e inequívoco do titular, nos termos do art. 7º, inciso I. Caberia apenas ao indivíduo autorizar a utilização dos seus dados pessoais devendo, o consentimento ser interpretado como uma expressão da autonomia da vontade. Assim, estaria assegurado ao indivíduo o poder de exercer um controle absoluto sobre as informações que lhe dizem respeito.

Ainda no que tange ao consentimento, é necessário ressaltar que deve ser fornecido por escrito fornecido por escrito ou por qualquer outro meio que o certifique, segundo o art. 9º. Ademais, o mesmo dispositivo estabelece uma hipótese *ope legis* de inversão do ônus da prova, ao dispor que cabe ao responsável comprovar que o consentimento foi obtido em conformidade com os requisitos da lei. A legislação em comento também veda autorizações genéricas para o tratamento de dados pessoais, sendo exigido que o consentimento se referira a finalidades determinadas, podendo, entretanto, ser revogado a qualquer momento.

Destaque-se, não se olvidou de abordar a questão dos dados sensíveis, de fundamental importância, tendo em vista o efeito devastador que o tratamento e a utilização de tais dados podem trazer para o seu titular, sobretudo quando utilizados para fins discriminatórios. Levando em consideração se tratarem de informações que só dizem respeito à própria pessoa, no âmbito mais reservado possível, o anteprojeto estabelece que, em regra, ninguém será obrigado a fornecer dados sensíveis, ficando proibida a formação de bancos de dados que contenham informações dessa natureza.

De acordo com o art. 15 do anteprojeto, o término do tratamento de dados ocorre quando atingir a sua finalidade ou os dados deixarem de ser necessários ou pertinentes para os fins a que se destinam, dentre outras hipóteses. Em regra, os dados pessoais devem ser eliminados após o término do seu tratamento, sendo permitida, porém, a sua transferência a

terceiros, desde que sejam utilizados para finalidade análoga àquela para a qual foram coletados.

A primeira versão do anteprojeto de lei de proteção de dados pessoais previa, no caput de seu art. 34, a obrigatoriedade de as entidades privadas de tratamento de dados pessoais com mais de duzentos empregados indicarem um responsável pelo tratamento, a quem caberia zelar, de forma independente, pela observância das disposições da lei. Machado (2015) critica esse dispositivo, que foi suprimido na nova versão, apresentada em outubro de 2015. No entendimento da autora:

> Não se compreende com base em que o legislador estipulou esse limite de empregados para que uma determinada empresa tenha um responsável pelos dados pessoais manuseados. Tal exigência não se revela adequada em razão do tipo de bem que se pretende tutelar, devendo-se incluir, todas as empresas com atuação no âmbito eletrônico, independente do número de colaboradores, considerando ainda as consequências advindas do tratamento dos dados pessoais. (MACHADO, 2015, p. 58-59)

No capítulo que trata dos direitos do titular dos dados pessoais, são garantidos os seus direitos fundamentais de liberdade, intimidade e privacidade. Conforme a dicção do art. 18, o indivíduo tem direito a obter, em relação aos seus dados: a confirmação da existência de tratamento, o acesso aos dados, a correção de dados incompletos, inexatos ou desatualizados, a eliminação, a qualquer momento, de dados pessoais com cujo tratamento o titular tenha consentido. Nessa perspectiva, percebe-se um grande passo da legislação brasileira rumo à consagração da autodeterminação informativa ao conferir aos cidadãos o direito material de controlar as informações que circulam a seu respeito nos mais diversos bancos de dados.

Vale destacar que, segundo o art. 50, os responsáveis pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas que estabeleçam condições de organização, normas de segurança, além de outros aspectos relacionados ao tratamento de dados pessoais. Por meio desses códigos de boas práticas, adaptados à realidade e às necessidades de cada setor, como o Código Brasileiro de Autorregulamentação para a Proteção aos Dados Pessoais apresentado pela ABEMD, pretende-se obter maior eficácia concreta das normas de proteção de dados previstas no anteprojeto.

Para a hipótese de infrações das normas previstas em lei, são estabelecidas sanções administrativas, a ser aplicadas pela Autoridade Garante, isolada ou cumulativamente, de acordo com as peculiaridades do caso concreto e com a gravidade e natureza das infrações, à natureza dos direitos pessoais afetados, à existência de reincidência, à situação econômica do

infrator e aos prejuízos causados. Dentre as sanções, dispostas no art. 52 do anteprojeto, se podem citar: multa simples ou diária, publicização da infração, bloqueio ou cancelamento dos dados pessoais, suspensão de operação de tratamento de dados pessoais ou de funcionamento de banco de dados.

Por fim, cabe ressaltar que a primeira versão do anteprojeto limitou-se a prever a criação e principais características do órgão competente pela implementação e fiscalização da lei de proteção de dados pessoais, deixando para outra legislação a sua estrutura e atribuições. Essa opção despertou críticas da doutrina, que defende que deixar para regular posteriormente esta estrutura significa atrasar mais ainda a concretização do direito à privacidade, considerando que o Brasil já inicia tardiamente a tutela específica de dados pessoais. (MACHADO, 2015)

De forma a sanar essa lacuna, a nova versão do anteprojeto estabelece a estrutura e as atribuições do órgão competente, o Conselho Nacional de Proteção de Dados e da Privacidade, nos moldes da Autoridade Garante prevista pelo Código Italiano. Esse órgão tem como principal característica a independência, como esclarece Machado (2015):

> O recurso à um órgão de fiscalização e controle, dotado de independência é uma prática bastante comum nos Estados democráticos. O ente estatal, não tendo mais condições de arcar com a responsabilidade pela fiscalização dos diversos serviços públicos postos à disposição do cidadão, bem como pela necessidade de se regular determinadas áreas do mercado, cria órgãos de controle e fiscalização. Pode-se citar como exemplo no Brasil, as chamadas agências reguladoras (...). Não se pretende afirmar que o órgão que compõe a Autoridade de Garantia seja uma agência reguladora, mas tão somente demonstrar as semelhanças entre ambas, já que têm funções de órgão controlador e fiscalizador. (MACHADO, 2015, p. 60)

Destarte, segundo o art. 53, o Conselho Nacional de Proteção de Dados e da Privacidade terá entre suas atribuições: zelar pela proteção dos dados pessoais, nos termos da legislação, elaborar diretrizes para uma Política Nacional de Proteção de Dados Pessoais e Privacidade, estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, elaborar relatórios anuais acerca de suas atividades e editar normas sobre proteção de dados pessoais e privacidade. Quanto à sua estrutura, o artigo seguinte estabelece que será composto por quinze representantes titulares e quinze suplentes designados pelo Ministro de Estado da Justiça, com mandato de dois anos, podendo ser renovado uma única vez por igual período, indicados pelos três poderes ou escolhidos entre representantes do setor privado, da academia e da sociedade civil.

CONCLUSÃO

A partir da análise da privacidade em diversos momentos históricos, pôde-se constatar que o seu surgimento está relacionado à conquista de um privilégio por parte de uma classe mais abastada da sociedade, e não realização de uma exigência natural de cada indivíduo. Além disso, a privacidade, em sua origem, guardava maior proximidade com a ideia de propriedade do que com a liberdade ou a autonomia dos indivíduos. Em outras palavras, o direito de propriedade era pré-requisito para que o indivíduo pudesse gozar de privacidade.

Com o tempo, e no mesmo compasso do desenvolvimento tecnológico, verificou-se a expansão do conceito de privacidade. Esta passou a ser associada à noção de que seria necessário garantir ao indivíduo meios de exercer o controle dos poderes baseados na utilização de informações a seu respeito, ou seja, o reconhecimento do direito à autodeterminação informativa.

Diante dessa nova realidade, os ordenamentos jurídicos tiveram que passar por adaptações a fim de garantir aos indivíduos a efetiva proteção de seus dados pessoais contra abusos perpetrados pelos responsáveis pelo tratamento. Merece destaque o modelo europeu de disciplina da matéria, sistemático, estruturado em torno de diretivas da União Europeia, tendo eleito como base a ideia de que a privacidade se reveste de natureza de direitos humanos, figurando como pressuposto do estado de direito.

O direito brasileiro, parecendo alheio às necessidades ditadas pelo atual grau de evolução tecnológica, permanece desprovido de lei específica sobre proteção de dados pessoais. Com o intuito de fomentar o debate sobre o tema e provocar o Congresso Nacional a corrigir essa lacuna, o Ministério da Justiça apresentou um Anteprojeto de Lei de Proteção de Dados Pessoais, que estabelece requisitos para o tratamento de dados pessoais, inspirado pela legislação italiana.

O anteprojeto de lei pretende a autodeterminação informativa dos cidadãos, dentre outras medidas, por intermédio do Conselho Nacional de Proteção de Dados e da Privacidade, órgão semelhante à Autoridade Garante italiana, a quem seria conferida a atribuição de zelar pela proteção dos dados pessoais. Ademais, estabelece princípios a serem observados pelos envolvidos na atividade de tratamento de dados pessoais, como o princípio da finalidade, da adequação, da necessidade, do livre acesso, da segurança e da não discriminação.

Em caso de violação desses princípios, de utilização ilícita ou inexata dos dados pessoais ou de desprezo das normas de segurança e de sigilo de dados previstas no anteprojeto

de lei, por exemplo, entende-se necessária a responsabilização civil objetiva dos responsáveis pelo tratamento de dados, que ficam obrigados ao ressarcimento de todos os danos decorrentes da atividade. Cabe ressaltar que a disciplina de responsabilidade objetiva se justifica pela dificuldade de demonstração do dano decorrente da violação da privacidade, além do fato de que a atividade de tratamento de dados pessoais tem natureza perigosa, em consonância com o disposto no Código Civil.

REFERÊNCIAS

Carta de Princípios para o Tratamento de Dados Pessoais (Minuta 01/12/2011). Disponível em: <http://www.abemd.org.br/interno/Carta_de_Principios.pdf>. Acesso em: 31 de mar. 2016.

Código Brasileiro de Autorregulamentação para a Proteção aos Dados Pessoais (Minuta 01/12/2011). Disponível em: <http://www.abemd.org.br/interno/Codigo_Autorreg_Dados Pessoaois.pdf>. Acesso em: 31 de mar. 2016.

COSTA JÚNIOR, Paulo José da. **O direito de estar só**: tutela penal da intimidade. São Paulo: Revista dos Tribunais, 1995.

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

_____. Um código para proteção de dados pessoais na Itália. In: **Revista Trimestral de Direito Civil**, Rio de Janeiro, v. 16, 2003.

_____. Responsabilidade Civil por Violação de Bancos de Dados. **In Revista Forense**. Rio de Janeiro, v. 105, n. 401, p. 677–691, jan./fev., 2009.

_____, VIOLA, Mario. Risco e Informação Pessoal: o Princípio da Finalidade e a Proteção de Dados no Ordenamento Brasileiro. In **Revista Brasileira de Risco e Seguro**. Rio de Janeiro, v. 5, n. 10, p. 85-102, out.2009/mar.2010.

Entenda o Marco Civil da Internet ponto a ponto. Disponível em: <http://www.ebc.com.br/tecnologia/2014/04/entenda-o-marco-civil-da-internet-ponto-a-ponto>. Acesso em: 29.03.2016.

GUERRA, Sidney. **O Direito à Privacidade na Internet**: uma Discussão da Esfera Privada no Mundo Globalizado. Rio de Janeiro: América Jurídica, 2004.

LAGES, Leandro Cardoso. **Direito do Consumidor**: a lei, a jurisprudência e o cotidiano. 2. ed., Rio de Janeiro: Lumen Juris, 2015

MACHADO, Joana de Moraes Souza. A Expansão do Conceito de Privacidade e a Evolução na Tecnologia de Informação com o Surgimento dos Bancos de Dados. In **Revista da AJURIS**, v. 41, n. 134, p. 337-363, jun.2014.

_____. A Tutela da Privacidade no Controle de Dados Pessoais no Direito Brasileiro. In: Arquivo Jurídico, Teresina, v. 2, n. 2, jul./dez. 2015, p. 43-65.

Projetos de Lei e Outras Proposições: PL 2126/2011. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=517255>. Acesso em: 29.03.2016.

RODOTÀ, Stefano. **A vida na sociedade de vigilância. A privacidade hoje**. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Doneda. Rio de Janeiro: Renovar, 2008.

SAMPAIO, José Adércio Leite. **Direito à Intimidade e à Vida Privada**: uma visão jurídica da sexualidade, da família da comunicação e informações pessoais. Belo Horizonte: Del Rey, 1998.