A PROTEÇÃO JURÍDICA DE DADOS PESSOAIS NA *INTERNET*: análise comparada do tratamento jurídico do tema na União Europeia e no Brasil.

THE JURIDICAL PROTECTION OF PERSONAL DATA ON INTERNET: comparative analysis of the theme's juridical treatment in the European Union and in Brazil.

Letícia Brum da Silva[1]
Rosane Leal da Silva[2]

RESUMO: O presente artigo trata da proteção de dados pessoais na *Internet*, partindo de um breve panorama sobre o tema e das situações de vulnerabilidade que podem se apresentar ao titular. Revelado o problema, apresenta-se o tratamento jurídico do tema na União Europeia, que se notabiliza por desde a década de oitenta possuir normativas sobre a proteção de dados pessoais. Em contrapartida a esse exemplo de proteção, apresenta-se o estado da questão no Brasil, com destaque ao Projeto de Lei n° 4.060/2012, atualmente em tramitação no Congresso Nacional. Para a elaboração deste artigo foi utilizado o método de procedimento comparativo, contrastando-se as Diretivas da União Europeia e o Projeto de Lei n° 4.060/2012, que visa a regulamentar a matéria no país. Ao destacar as principais semelhanças e diferenças entre as regulamentações, conclui-se que o projeto de legislação brasileira se mostra insuficiente e fora dos padrões de segurança estabelecidos pela União Europeia, pioneira na produção de normas para tutelar os dados pessoais de seus cidadãos.

Palavras-chave: *Internet*; Dados pessoais; Diretivas da União Europeia; Projeto de Lei n° 4.060/2012; Direitos fundamentais.

ABSTRACT: The present paper addresses the personal data protection on *Internet*, starting from brief scenery on the theme and the situations of vulnerability which may be presented to the user. The problem revealed then there is the European Union's juridical treatment, that has the distinction of having guidelines about the personal data protection since the 80's. Opposing to this example of protection, there is the situation in Brazil, highlighting the Bill n° 4.060/2012, currently to be passed in the National Congress. It was used the comparative procedure methodology to write this paper, comparing the European Union Guidelines and the Bill n° 4.060/2012 which aims to regulate this subject in the country. When highlighting the main similarities and differences between both guidelines, it is possible to conclude that

[1] Acadêmica do Curso de Direito no Centro Universitário Franciscano (UNIFRA). E-mail para contato: leticiabrum.dto@hotmail.com
[2] Doutora em Direito pela Universidade Federal de Santa Catarina (UFSC). Professora Adjunta do Curso de Direito da Universidade Federal de Santa Maria, com atuação na graduação e mestrado. Professora do Centro Universitário Franciscano, ambos em Santa Maria (RS). Líder do Grupo de Pesquisa Teoria Jurídica no Novo Milênio (UNIFRA) e Núcleo de Direito Informacional (UFSM). E-mail para contato: rosaneleals@terra.com.br

the Brazilian Bill is not enough and does not match the safety standards established by the European Union, pioneer in producing guidelines to protect the personal data of its citizens.

Key-words: *Internet*; Personal data; European Union guidelines; Bill n° 4.060/2012; Fundamental rights.

INTRODUÇÃO

O crescente uso das tecnologias da informação e da comunicação, em especial da *Internet*, imprimiu maior dinamicidade às relações econômicas, à participação política e às interações sociais, redesenhando as formas de *ser* e *estar* no mundo. Em nenhum outro momento histórico foi tão fácil e rápido acessar informações, produzir e compartilhar conteúdos, comunicar e interagir em *sites* de redes sociais, *blogs* e *microblogs*, tudo de maneira instantânea.

O intenso desenvolvimento capitaneado pelo segmento de Tecnologias da Informação (TI) acelera ainda mais esse processo, pois a cada dia são lançados no mercado novos equipamentos, aplicativos, plataformas e ferramentas que maximizam a experiência de navegação na *web*, o que faz com que um número crescente de pessoas almeje a inclusão digital.

Mas ao lado desse panorama de otimismo e de novas oportunidades também se revelam inéditos problemas e desafios decorrentes do grande fluxo informacional, especialmente quando as informações assumem a forma de dados pessoais e saem do controle do seu titular. Essa situação de vulnerabilidade tanto pode ocorrer quando os dados são espontaneamente disponibilizados nas interações sociais, como ocorre com publicações feitas em *sites* de redes sociais; nos casos em que são recolhidos pelo fornecedor para permitir a abertura de contas que garantirão o acesso a serviços e produtos ou nas situações de captura indevida por meio de algum programa espião. A pluralidade de formas de recolhimento de informações demonstra a complexidade do tema, pois mesmo o internauta mais cauteloso e com seletivas atuações no ambiente virtual não fica a salvo de sofrer ataques aos seus dados pessoais.

O interesse no estudo do tema se aprofunda na medida em que o aumento no número de internautas no Brasil não é acompanhado da implementação de mecanismos hábeis à proteção do usuário, o que conduz ao seguinte problema: considerando o processo de inclusão digital e o recente Projeto de Lei sobre dados pessoais, enviado ao Congresso Nacional, é possível afirmar que a proposta brasileira é adequada e suficiente para responder aos desafios

da sociedade informacional? O referido Projeto encontra-se alinhado com Estados que há mais tempo estão integrados à sociedade informacional, a exemplo do que ocorre na União Europeia?

Objetivando suscitar o debate e responder a essas indagações apresenta-se este artigo, elaborado com emprego do método de abordagem dedutivo, utilizado para analisar o tratamento dos dados pessoais na *Internet* e identificar situações de risco e vulnerabilidade ao internauta. Partindo-se dessa abordagem geral e considerando que o Brasil ainda não reconheceu os dados pessoais e o direito à autodeterminação informativa como direitos fundamentais e levando em conta que o país ainda não dispõe de legislação infraconstitucional específica sobre o tema, buscam-se elementos de análise no Direito comparado, notadamente na legislação da União Europeia. Para investigar o tratamento jurídico existente foram examinados documentos oficiais relacionados à proteção de dados pessoais, disponibilizados no *site* da União Europeia. Uma vez identificadas as normativas, aplicou-se o método de procedimento comparativo, o que permitiu contrastar o conteúdo das Diretrizes europeias com o Projeto de Lei de Proteção aos Dados Pessoais brasileiro, enviado em 2012 ao Congresso Nacional, atualmente em tramitação sob o n° 4.060, tarefa empreendida com o objetivo de responder ao problema de pesquisa acima explicitado.

1 OS DADOS PESSOAIS COMO UMA NOVA CATEGORIA DE DIREITOS FUNDAMENTAIS.

A implantação da *Internet* no Brasil ocorreu a partir do Projeto da Rede Nacional de Pesquisa - RNP, criado em 1989 pelo Ministério da Ciência e Tecnologia (MCT), com apoio de instituições governamentais de vários Estados, entre as quais a Fundação de Amparo à Pesquisa do Estado de São Paulo (TAKAHASHI, 2010). Entretanto, somente a partir de 1995 a rede brasileira ultrapassou os muros das academias e centros de pesquisa, estendendo-se aos usuários individuais e empresas. No mesmo ano foi criado o Comitê Gestor da *Internet* no Brasil (CGI.br), órgão encarregado de elaborar programas e projetos voltados à implantação da *Internet* no país (CGI.BR, 2012).

O crescente número de pessoas conectadas à *Internet* exigiu o mapeamento da inclusão digital no país, atividade que passou a ser desenvolvida pelo Centro de Estudos sobre as Tecnologias da Informação e da Comunicação (CETIC.br), um dos braços executivos do CGI.br. O CETIC realiza pesquisas sistemáticas por meio das quais mapeia a utilização das tecnologias da informação e comunicação em diversos segmentos, como domicílios,

empresas, telecentros e governo eletrônico[3], bem como produz e divulga indicadores, estatísticas e informações estratégicas sobre o desenvolvimento da *Internet* brasileira. Tais indicadores permitem mapear os usos e obstáculos que os brasileiros enfrentam quando utilizam as tecnologias da informação e comunicação.

As informações colhidas na "TIC Domicílios E TIC empresas" contribuem para monitorar e avaliar o impacto socioeconômico das NTICs[4], em especial a *Internet*, promotora de verdadeira revolução informacional. Essa revolução conduz a transformações no próprio conceito de informação, ampliando-o consideravelmente para abarcar imagens, sons, vídeos ou outros formatos, que passam a integrar grandes fluxos informacionais facilmente armazenáveis. Esses fluxos podem ser manipulados/tratados e transmitidos de maneira imediata e planetária, fenômeno de grande impacto nos segmentos econômico, social e político, o que culmina por determinar o próprio modelo de sociedade, que passa a ser cada vez mais interconectada, em rede, verdadeira sociedade informacional[5].

Sob o signo do desenvolvimento tecnológico acelerado a cada dia são lançados novos aplicativos e criadas ferramentas e ambientes virtuais para encantar um público que não cessa de crescer. E, seduzidos pelas novas oportunidades de interconexão, os internautas (especialmente os brasileiros) revelam-se assíduos utilizadores de *sites* de redes sociais[6],

---

[3] Para Rover (2006, p. 99), "Governo eletrônico é uma infra-estrutura única de comunicação compartilhada por diferentes órgãos públicos a partir da qual a tecnologia da informação e da comunicação é usada de forma intensiva para melhorar a gestão pública e o atendimento ao cidadão. Assim, o seu objetivo é colocar o governo ao alcance de todos, ampliando a transparências das suas ações e incrementando a participação cidadã".

[4] Denominam-se Novas Tecnologias de Informação e Comunicação (NTICs) as tecnologias e métodos para comunicar surgidas no contexto da Revolução Informacional, "Revolução Telemática" ou Terceira Revolução Industrial, desenvolvidas gradativamente desde a segunda metade da década de 1970 e, principalmente, nos anos 1990. A imensa maioria delas se caracteriza por agilizar, horizontalizar e tornar menos palpável (fisicamente manipulável) o conteúdo da comunicação, por meio da digitalização e da comunicação em redes (mediada ou não por computadores) para a captação, transmissão e distribuição das informações (texto, imagem estática, vídeo e som). Atualmete as TICs são difundidas pelo mundo e abrangem alternativas, que passam pelos jornais, rádios, televisões, ingressando pela cibernética, a qual universaliza qualquer informação, principalmente através da *Internet* (COELHO, 2010).

[5] Nesse sentido, observa-se a inexistência de um consenso acerca da expressão terminológica mais adequada para definir esse novo modelo social, de modo que é possível encontrar outras denominações, tendo em vista o contexto histórico em que são utilizadas e dependendo do autor que a emprega. Não obstante os termos "sociedade da informação" e "sociedade informacional" serem utilizados frequentemente como sinônimos, Castells (2008, p. 64-65) é um dos poucos autores que faz evidente distinção conceitual. Para este autor, o termo sociedade informacional indica uma forma específica de sociedade, na qual a "geração, o processamento e a transmissão da informação tornam-se as fontes fundamentais de produtividade e poder devido às novas condições tecnológicas surgidas nesse período histórico".

[6] Com base em Recuero (2009, p. 102) pode-se dizer que os sites de redes sociais são *softwares* sociais com aplicação diretamente voltada à comunicação mediada pelo computador, que oferecem a possibilidade de construção de uma "persona" pelo perfil do usuário ou por sua página pessoal, promovendo a interação dos indivíduos através de comentários e a exposição pública de cada ator na rede social que integra.

blogs e *microblogs*[7], nos quais disponibilizam e divulgam voluntariamente suas informações pessoais, sem se preocupar com quem irá acessá-las ou para qual finalidade serão utilizadas.

Com efeito, na sociedade informacional os próprios titulares dos dados pessoais[8] conscientemente os disponibilizam para a abertura das contas que lhes permitirão o acesso aos serviços de *Internet* e, a partir daí, passam a expor inúmeras informações. A vulnerabilidade ocorre de maneira imediata, pois basta acessar um *site* de rede social (como o *Facebook*) para que os dados pessoais do internauta tais como nome, fotos, estado civil, opção religiosa e muitos outros dados sejam facilmente visualizados e compartilhados por seus contatos e até mesmo por terceiros, sequer conhecidos do internauta. Outra situação recorrente ocorre quando algum contato da rede social faz uma postagem e nela publica imagens, comentários e informações sobre algum amigo, também integrante da mesma rede, que vê alguns de seus dados divulgados sem sua autorização.

Além disso, por se tratar de tecnologia recentemente incorporada na vida dos brasileiros, muitas vezes o titular não percebe o grau de risco a que se expõe diante de determinados usos que faz das tecnologias da informação, especialmente quando divulga dados pessoais sensíveis.

Ao tratar do tema, De La Cueva (1993, p. 69-70) enfatiza a importância dessa espécie de dados, ao afirmar que eles se ligam ao núcleo da personalidade e dignidade humanas, o que os torna "objeto de garantía sustantiva a través de otros derechos fundamentales". E não poderia ser diferente, já que tais dados podem referir-se a questões como crença e opção religiosa, ideologia e opiniões políticas, origem racial, condições de saúde e detalhes mais íntimos da vida da pessoa, como por exemplo, sua orientação sexual. Por este motivo, sua tutela deve ser especial, destinando-se tratamento mais severo a quem os manipula ou utiliza sem a devida autorização, pois a divulgação a terceiros pode gerar danos ainda maiores e por vezes irreparáveis a seus titulares.

---

[7] *Microblogs* são espécies de *blog* que permitem atualizações por vários meios, como SMS, *Messenger*, *Skype*, e-*mail* mp3 e *web*, de conteúdo compacto – até 140 caracteres. Segundo Comm (2009, p. 21), o *Twitter* é o mais popular, tendo sido lançado em 2006, pelos programadores Evan Williams, Jack Dorsey e Biz Stone. Sua grande característica é a simplicidade, pois apesar de contar com muitas ferramentas adicionais, seu objetivo precípuo é estabelecer um canal de comunicação onde o usuário possa, em 140 caracteres, dizer o que está fazendo naquele momento.

[8] Apesar das divergências entre os autores, neste trabalho empregar-se-á a definição de dados pessoais oferecida por Castro (2005, p. 70-88), segundo a qual dados pessoais compreendem qualquer informação (numérica, alfabética, gráfica, fotográfica, acústica), independente do suporte (som e imagem), referente a uma pessoa identificada ou identificável. Assim, integram esse conceito informações como o número de identidade, CPF, endereço, número do cartão de crédito, fotos, dados de consumo, entre outras.

Portanto, deve haver cautela redobrada quando se trata de dados sensíveis, seja no momento do recolhimento, seja quanto à segurança em seu armazenamento, a fim de garantir que seu uso não se dissocie da finalidade para a qual foi obtida. Esse cuidado é necessário porque, segundo Limberger (2009), proteger os dados sensíveis é uma forma de prevenir ou eliminar a discriminação, o que por certo contribuirá para a efetivação do princípio constitucional da igualdade, consagrado no art. 5° da Constituição Federal, segundo o qual são vedadas as diferenciações arbitrárias e discriminações[9].

Observa-se que a necessidade em proteger juridicamente o cidadão resulta do fato de que os dados pessoais adquiriram nos últimos anos forte componente econômico devido à possibilidade de sua comercialização, o que atrai empresas e fornecedores que atuam no ambiente virtual a utilizarem as mais variadas estratégias para obter dados dos internautas. Com efeito, os dados pessoais de um consumidor traduzem aspectos de sua personalidade e revelam comportamentos e preferências, tornando-o um alvo fácil de mensagens publicitárias. Quando se trata da *Internet* o tema ganha inda mais interesse tendo em vista a possibilidade de criação de perfis psicológicos que revelam os hábitos de consumo, os gostos e preferências do indivíduo e, uma vez formado o perfil, posteriormente esse consumidor passa a ser alvo de publicidades indesejadas, *e-mails* que oferecem serviços, produtos e uma série de outras "promoções" que parecem elaboradas e direcionadas especialmente a ele, tudo articulado com base nos dados antes recolhidos. Percebe-se, pois, que as novas tecnologias informacionais, especialmente a *Internet*, convertem a informação em uma riqueza fundamental da sociedade, o que acentua a necessidade de sua proteção.

Considerando as características da sociedade informacional, os novos hábitos de consumo e de interação social, adquiridos em virtude da crescente inclusão digital ocorrida nos últimos anos no Brasil[10] alguns autores[11] passaram a defender a emergência do direito

---

[9] Uma das formas prejudiciais de utilização de informações e, consequentemente, violação deste princípio consagrado na Carta Magna seria o caso em que um banco de dados que contém informações sobre a religião, sexo ou saúde de uma pessoa identificável os concedesse a determinada empresa e assim criasse uma situação de desigualdade. Outro exemplo dessa situação seria a hipótese de um trabalhador, portador do vírus HIV, que não é contratado ou é despedido em virtude da doença. Seria uma situação de nítida desigualdade, pois a possibilidade de a empresa escolher um trabalhador saudável, na contratação, é muito grande, o que configuraria uma discriminação para com o portador da doença, cujos dados sensíveis foram indevidamente divulgados. Por este motivo, é restrito o número de atividades profissionais que podem solicitar o exame HIV, pois, primeiramente, deve-se ponderar a proteção individual do trabalhador com o risco de expor a saúde da coletividade, demonstrando-se assim, que a divulgação de dados sensíveis pode gerar situações de discriminação e prejuízos a seus titulares.

[10] Segundo dados revelados pelo CETIC na última edição da pesquisa TIC Domicílios, aproximadamente 45% da população brasileira com mais de 10 anos de idade é usuária da *Internet*, o que apresenta variações de região a região: a região sudeste registrou 53% dos moradores com acesso a essa tecnologia; região Centro-Oeste (51%); região Sul (50%), Região Norte (36%) e região Nordeste (32%). A conexão por domicílio é menor e segundo

sobre a proteção de dados pessoais como categoria jurídica autônoma, merecedora do mesmo *status* dos demais direitos fundamentais. Defendem também a necessidade de reconhecimento do direito à autodeterminação informativa[12] por parte do titular dos dados, a partir da qual o internauta deve ter a garantia de controlar *como* e *quando* suas informações serão recolhidas e utilizadas, determinar quem terá acesso a seus dados pessoais e como eles serão armazenados e tratados (PEREIRA, 2005).

Por meio dessa nova perspectiva busca-se conferir maior poder e controle do titular sobre seus dados, na tentativa de conciliar o uso da *Internet* (e a grande disponibilização de dados pessoais) com níveis compatíveis de proteção a direitos fundamentais, como a intimidade[13] e a privacidade[14]. Trata-se, em outras palavras, de compreender que embora o ciberespaço historicamente tenha sido identificado como um ambiente propício para o exercício das liberdades, essa liberdade não é absoluta e toda a vez que o particular (pessoa física ou empresa) ou o próprio Estado expuserem dados pessoais de outros devem ser responsabilizados por eventuais danos causados ao titular.

Entende-se que a adoção de tal posição não se constitui afronta arbitrária ao exercício das liberdades ou censura prévia, pois a imposição de limites é necessária para assegurar o próprio sistema de liberdades, pilar do Estado Democrático de Direitos. Essa posição, por vezes veementemente repudiada por vários doutrinadores, encontra amparo nas lições de Pérez Luño (2011, p. 303), para quem já é hora de superar a inocência do "[...] idílico 'estado de naturaleza' de libertad sin restricciones de Internet, las circunstancias aconsejan remediar los peligros del desorden mediante soluciones jurídicas".

---

estimativa da União Internacional de Telecomunicações (UIT), 38% dos lares brasileiros possuem acesso à *Internet*, o que coloca o Brasil abaixo da média das Américas, que registram índices de 50% de domicílios com conexão (PESQUISA, 2012, p. 154-160).

[11] Um dos precursores dessa posição é o doutrinador Antônio Henrique Pérez Luño, para quem a autodeterminação informacional protege a intimidade a partir do direito de defesa e de controle sobre o fluxo de dados pessoais, na esteira da qual os demais direitos (honra e imagem) também estariam protegidos (PÉREZ LUÑO, 2005, p. 335-339).

[12] Este conceito compreende uma série de direitos, tais como: a) direito de não ser transparente; b) de ser deixado em paz; c) direito de ter autonomia de escolha para quem disponibilizar informação e ter controle sobre seus dados pessoais; d) poder de defesa da pessoa contra as ações do Estado e dos particulares.

13 Ao observar a bibliografia sobre o tema nota-se a existência de divergências no tratamento da intimidade e da privacidade. Pereira (2006) entende haver diferença entre intimidade e privacidade, pois para este autor enquanto a primeira se relaciona à esfera mais reservada, ligando-se às emoções, pensamentos e ideias mantidas numa zona nuclear, o direito à privacidade abarca aspectos da convivência familiar e de um pequeno grupo de amigos. Já a privacidade é mais ampla e abarca um número maior de pessoas (amigos, familiares) e sofre variações do seu conteúdo, daí a dificuldade em determinar o âmbito e o alcance desse direito (PEREIRA, 2006, p. 116).

[14] Silva (2009, p. 206) entende que a privacidade, concebida em seu sentido lato, pode ser interpretada como o "conjunto de informação acerca do individuo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem a isso poder ser legalmente sujeito". Por outro lado, Ferreira Filho (1999) observa que a intimidade é a vida em ambiente de convívio, no interior de um grupo fechado e reduzido, normalmente, ao grupo familiar.

Além de reconhecer que o ambiente virtual precisa submeter-se a alguma forma de regulação, Pérez Luño (2005, p. 339) também oferece rica contribuição para pensar o tratamento dos direitos em tempos de Internet. Para este teórico, os direitos fundamentais diretamente relacionados com a personalidade da pessoa (como honra, nome, imagem, privacidade, intimidade) não podem ser vistos como categorias estanques e dissociadas, merecendo ser tutelados a partir de uma perspectiva unitária, que considera a multiplicidade das interações e conexões sociais do seu titular. Defende, portanto, a necessidade de se reconhecer o direito à autodeterminação informativa, de escopo mais abrangente, como uma categoria de direito fundamental.

Diante disso, revela-se a necessidade de também acolher e considerar juridicamente os dados pessoais como uma nova categoria de direito fundamental, categoria esta que emerge com o intuito de ampliar a proteção dos usuários, tendo como escopo a proteção da dignidade de pessoa humana.

Essas contribuições teóricas suscitam grande interesse, sobretudo para refletir sobre o tratamento dos direitos fundamentais no Brasil. Assim, no ano em que a Carta Constitucional brasileira completa vinte e cinco anos mostra-se oportuno e necessário trazer à discussão a ampliação do rol de direitos fundamentais, de modo a abarcar aqueles decorrentes do intenso desenvolvimento tecnológico experimentados nos últimos anos, notadamente na área da informação e comunicação. Essa reflexão não pode mais ser postergada, sobretudo porque o tratamento de dados pessoais na *Internet* oferece uma série de riscos ao seu titular, com claro potencial para fomentar discriminações e preconceitos de origem, raça, sexo, cor, idade, o que por certo viola a dignidade humana.

O reconhecimento de novas categorias de direitos fundamentais, como os dados pessoais e a autodeterminação informativa, revela-se medida necessária não só para a concretização dos objetivos da República Federativa do Brasil, elencados no art. 3º da Carta Magna, como também para o alinhamento jurídico do país aos demais Estados que já adotaram igual postura em favor da dignidade da pessoa, a exemplo da União Europeia. Com efeito, enquanto a discussão sobre o tema é ainda incipiente no Brasil, a União Europeia se preocupa com a tutela desse direito desde 1995, momento em que os Estados integrantes perceberam a necessidade de garantir um adequado grau de proteção aos dados pessoais dos usuários das novas tecnologias, tratando-os como direitos fundamentais.

Considerando a incipiência do tratamento do tema no Brasil em comparação com a experiência europeia[15], no próximo tópico serão apresentadas as principais iniciativas desenvolvidas por aqueles Estados Membros, o que oferecerá subsídios para posteriormente analisar criticamente a posição brasileira.

2 A PROTEÇÃO JURÍDICA DOS DADOS PESSOAIS NA UNIÃO EUROPEIA: o exemplo dos países integrados na sociedade informacional.

A preocupação com a proteção das pessoas frente ao desenvolvimento da sociedade informacional é um tema que há muitos anos preocupa a União Europeia[16], encontrando-se registros de compromissos firmados ainda na década de oitenta, com destaque para a Convenção para a proteção de pessoas frente ao tratamento automatizado dos dados de caráter pessoal (MATTELART, 2002, p. 124).

Os anos subsequentes demostraram que essa preocupação tinha reais fundamentos e que realmente havia a necessidade de assegurar um nível adequado de proteção à privacidade e as liberdades dos cidadãos no que concerne a seus dados pessoais, o que deveria ocorrer de forma equilibrada e homogênea nos Estados Partes. Em esforço conjunto, o Parlamento e o Conselho Europeu editaram a Diretiva 95/46/CE[17], em 24 de outubro de 1995 (COUTO, 2006).

A Diretiva merece destaque, tendo em vista ser o principal instrumento de proteção de dados, constituindo-se a base sobre a qual estão dispostas todas as normativas posteriormente elaboradas para a proteção de dados pessoais dos integrantes da União Europeia. Outro fator que a notabiliza é o fato de seu texto ter resultado de discussões e experiências nacionais[18] sobre a regulação da proteção de dados que datam da década de 1970 (DEBATE, 2011), motivos que justificam a apresentação de suas principais disposições.

---

[15] Segundo dados da União Internacional de Telecomunicações (UIT), desde 2005 tem aumentado o número de internautas na Europa que registrou, em 2011, 34 pontos acima da média brasileira (PESQUISA, 2011, p. 154).

[16] Como é sabido, a União Europeia como atualmente conhecida, é constituída em 25 de Março de 1957, por meio do Tratado de Roma, que formaliza o surgimento da Comunidade Econômica Europeia (CEE), constituída por alguns Estados Europeus que se unem para fazer frente aos desafios econômicos, políticos e sociais do período. (CASELLA, 1994).

[17] Os dados completos sobre essa Diretiva e as demais trabalhadas no texto encontram-se nas referências, ao final do artigo.

[18] Ao tratar da legislação acerca da proteção de dados pessoais, salienta-se que a primeira iniciativa Constitucional, no sentido de garantir proteção à intimidade frente ao uso da informática veio de Portugal, país-membro da União Europeia, que regulamentou a matéria no art. 35[18] de sua Carta Magna (PEREIRA, 2006). Eis a redação do referido artigo: Art. 35. 1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua *rectificação* e *actualização*, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.

Inicialmente a Diretiva apresenta seu objeto e definições importantes, dentre elas o conceito de dados pessoais, assim considerados qualquer informação relativa a uma pessoa singular identificada ou identificável. Pelos termos do documento, dado pessoal é toda a informação que possa identificar direta ou indiretamente uma pessoa, quer seja através de referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social.

Além disso, observa-se que o tratamento[19] de dados pessoais só será abrangido pela Diretiva quando utilizados meios totais ou parcialmente automatizados ou quando os dados estivessem contidos ou destinados a ficheiros[20] estruturados segundo critérios específicos relativos às pessoas.

No que tange à proteção dos dados pessoais, a referida Diretiva determinava que os Estados Membros especificassem as condições em que seria lícito o seu tratamento, observando-se sempre a tutela das liberdades e dos direitos fundamentais dos indivíduos.

Ademais, a Diretiva estabelecia princípios mínimos para possibilitar o tratamento de dados pessoais, dentre eles: a) que os dados pessoais só seriam recolhidos se houvesse uma finalidade legítima, determinada e explícita; b) os dados não poderiam ser utilizados para finalidade distinta da qual foram recolhidos; c) o recolhimento e tratamento dos dados dependem do consentimento inequívoco do seu titular.

Cabe salientar que essa Diretiva da década de noventa já previa a proteção especial para os chamados dados sensíveis, proibindo em seu art. 8°, 1, o tratamento de dados pessoais que revelassem origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, filiação sindical, dados relativos à saúde[21] e vida sexual ou qualquer outra

---

[19] Conforme o art. 2°, b, da Diretiva 95/46/CE, tratamento de dados pessoais é qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, registro, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição.

[20] Conforme expresso no art. 2°, c, da Diretiva 95/46/CE, ficheiro de dados pessoais é qualquer conjunto estruturado de dados pessoais, acessível segundo critérios determinados, que seja centralizado, descentralizado ou repartido de modo funcional ou geográfico.

[21] A exposição de dados pessoais e informações referentes à saúde de outrem foram inclusive objeto de discussão jurisprudencial no Caso Lindqvist, julgado pelo Tribunal de Justiça da União Europeia em 06 de novembro de 2003. Trata de decisão em ação contra Bodil Lindqvist, responsável pela criação de um *site* no qual divulgou informações suas e de dezoito outros membros da paróquia onde exercia as funções de catequista, dando ao conhecimento público fatos e situações familiares e de saúde de alguns paroquianos. O Tribunal de Justiça da UE aplicou a Diretiva 95/46/CE, entendendo que a referida normativa não oferecia, por si só, uma restrição ao princípio geral da liberdade de expressão, mas que as autoridades jurisdicionais nacionais deveriam aplicá-la de maneira proporcional e equilibrada, de maneira a tutelar dados pessoais de outro sem, todavia, limitar demasiadamente a liberdade dos outros usuários da rede, sob pena de se constituir em excessiva limitação ao sistema de liberdades (PÉREZ LUÑO, 2011, p. 312-316).

informação que pudesse gerar discriminação ou problemas ao seu titular, ficando a salvo determinadas situações excetuadas[22] pela normativa.

Outro ponto de destaque dessa Diretiva é que ela já previa a possibilidade de o titular do dado pessoal alterar e corrigir suas informações, bem como suspender o consentimento conferido para seu uso (COUTO, 2006), o que já sinalizava em direção ao princípio da autodeterminação informativa.

Da mesma forma, os itens 1 e 2 do art. 17 da Diretiva estabeleciam que o responsável pelo tratamento devesse pôr em prática medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição acidental ou ilícita, a perda acidental, a alteração, a difusão ou acesso não autorizados por terceiros, nomeadamente quando o tratamento implicar a sua transmissão por rede. Nesses casos competia aos Estados Partes adotar providências coercitivas para que o disposto nesse artigo fosse observado.

> Cônscios dos riscos que envolvem a atividade e do rápido desenvolvimento tecnológico, os Estados membros se comprometeram em adotar medidas capazes de assegurar um nível de segurança adequado em relação perigos que o tratamento apresenta considerando a natureza dos dados a proteger[23]. Para acompanhar a atuação das empresas do segmento a Diretiva 95/46/CE previu a criação de uma entidade especializada em todos os Estados membros, com a competência de fiscalizar e aplicar as disposições legais sobre dados pessoais, denominada de autoridade de controle[24].

---

[22] Artigo 8, 2: O nº 1 não se aplica quando:
a) A pessoa em causa tiver dado o seu consentimento explícito para esse tratamento, salvo se a legislação do Estado-membro estabelecer que a proibição referida no nº 1 não pode ser retirada pelo consentimento da pessoa em causa; ou
b) O tratamento for necessário para o cumprimento das obrigações e dos direitos do responsável pelo tratamento no domínio da legislação do trabalho, desde que o mesmo seja autorizado por legislação nacional que estabeleça garantias adequadas; ou
c) O tratamento for necessário para proteger interesses vitais da pessoa em causa ou de uma outra pessoa se a pessoa em causa estiver física ou legalmente incapaz de dar o seu consentimento; ou
d) O tratamento for efetuado, no âmbito das suas atividades legítimas e com as garantias adequadas, por uma fundação, uma associação ou qualquer outro organismo sem fins lucrativos de caráter político, filosófico, religioso ou sindical, na condição de o tratamento dizer unicamente respeito aos membros desse organismo ou às pessoas que com ele mantenham contactos periódicos ligados às suas finalidades, e de os dados não serem comunicados a terceiros sem o consentimento das pessoas em causa; ou
e) O tratamento disser respeito a dados manifestamente tornados públicos pela pessoa em causa ou for necessário à declaração, ao exercício ou à defesa de um direito num processo judicial.

[23] Se ainda assim houver dano, a Diretiva prevê que o responsável pelo tratamento poderá ser parcial ou totalmente exonerado desta responsabilidade se provar que o fato causador do dano não lhe é imputável. Contudo, os Estados-membros tomarão as medidas adequadas para assegurar a plena aplicação das disposições constantes na Diretiva e determinarão, nomeadamente, as sanções a aplicar em caso de violação das disposições adotadas nos termos da diretiva (art. 24).

[24] Conforme o art.28 da Diretiva 95/46/CE, cada Estado-membro estabelecerá que uma ou mais autoridades públicas serão responsáveis pela fiscalização da aplicação das disposições adotadas pelos Estados-membros

> Resta claro, portanto, que desde os anos iniciais da sociedade informacional os Estados que à época integravam as Comunidades Europeias, hoje União Europeia, empreendiam esforços no campo normativo para harmonizar suas legislações com vistas a tutelar os cidadãos, tanto na transmissão de dados e fluxos informacionais entre Estados Partes quanto destes com outros Estados não integrantes da União Europeia. Tal exigência já se apresentava na Diretiva 95/46/CE, que adotou o princípio da proteção adequada[25] (*adequate protectio*), segundo o qual para a realização de transações comerciais o Estado tem que possuir a certificação de que é um país com o nível de proteção de dados pessoais compatível com o existente na União Europeia.

Ressalta-se que esta adequação não é obrigatória, mas quando exigida se apresentava na forma de cláusulas contratuais modelo[26] elaboradas periodicamente pela Comissão Europeia, sendo aplicáveis a contratações com países que não integravam aquela Comunidade e não possuíam a certificação conferindo adequado nível de proteção de dados pessoais (REINALDO FILHO, 2005).

Tratando sobre o tema, Demócrito Reinaldo Filho (2005) entende que apesar de a adoção das cláusulas se revestirem de voluntariedade, sua observância e aplicação representa um meio para que empresas e organizações atendessem as exigências da Diretiva quanto a dados pessoais transferidos a países "não membros" que ainda não detivessem o reconhecimento de "proteção adequada".

Posteriormente, em 15 de dezembro de 1997 foi editada a Diretiva 97/66/CE, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das telecomunicações, também denominada "Diretiva Dados Pessoais nas Telecomunicações". Este documento visava preservar os princípios já estabelecidos pela Diretiva anterior, a partir da qual foram ampliadas as proteções, abarcando o setor das telecomunicações, não contemplado anteriormente.

---

no seu território. Essas autoridades, denominadas autoridades controladoras, exercerão com total independência as funções que lhes forem atribuídas.

[25] Artigo 25º,1: Os Estados-membros estabelecerão que a transferência de dados pessoais objeto de tratamento para um país terceiro, ou que se destinem a ser objeto de tratamento após a sua transferência, só pode realizar-se se o país terceiro em questão assegurar um nível de proteção adequado e compatível com o adotado na União Europeia.

2. A adequação do nível de proteção oferecido por um país terceiro será apreciada em função de todas as circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados; em especial, serão tidas em consideração a natureza dos dados, a finalidade e a duração do tratamento ou tratamentos projetados, os países de origem e de destino final, as regras de direito, gerais ou setoriais, em vigor no país terceiro em causa, bem como as regras profissionais e as medidas de segurança que são respeitadas nesse país.

[26] A Comissão Europeia elabora modelos de cláusulas contratuais para serem utilizadas por empresas e controladores de bancos de dados europeus que transfiram informações para outros países, quando estes não possuam sistema de nível adequado na proteção de dados pessoais (REINALDO FILHO, 2005).

Na esteira desta normativa, os Estados Europeus buscaram estender a proteção para o âmbito das instituições e órgãos comunitários. Para tanto publicaram o Regulamento n° 45, de dezembro de 2000, relativo à proteção das pessoas singulares cujos dados pessoais fossem recolhidos e tratados por instituições ou órgãos comunitários. Assim, o escopo da proteção conferida pela Diretiva 95/46/CE é ampliado por força do referido Regulamento, mantendo-se o mesmo âmbito de incidência, pois o cidadão cujos dados fossem recolhidos e tratados por órgãos comunitários gozariam da mesma tutela antes conferida.

Já em 2002 editou-se a Diretiva n° 58, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas, denominada "Diretiva Dados Pessoais nas Comunicações Eletrônicas". Esse documento se constitui em um marco, pois ele se dirige especificamente às comunicações eletrônicas.

Observa-se que a estrutura empreendida na citada Diretiva, bem como nas demais, observa os padrões da primeira: inicialmente apresenta o objeto e a abrangência[27] da Diretiva, seguida de algumas definições conceituais. Contudo, as principais inovações em relação à Diretiva 97/66/CE referem-se ao tratamento dos "*spams*" [28] e "*cookies*" [29]. No que concerne ao primeiro problema, a solução encontrada foi de que as mensagens só poderiam ser enviadas a quem expressamente tivesse aceitado ou quando houvesse uma relação comercial anterior à Diretiva que autorizasse o seguimento no envio do *spam* a utilizadores antigos. No segundo caso, a utilização dos *cookies* seria permitida desde que previamente o internauta destinatário fosse informado sobre seu envio e dos seus propósitos.

Comentando a referida Diretiva, Couto (2006) ressalta que esse documento inova ao incluir a regulamentação de dados do titular em listas públicas de serviços móveis ou fixos, cabendo ao interessado solicitar que seu nome fosse excluído da listagem.

A dinamicidade do tema, diretamente relacionado e impactado pelo rápido desenvolvimento das tecnologias da informação e comunicação, determinou a inserção de inovações no tratamento da matéria, o que foi feito por meio da Diretiva 2006/24/CE. Esse documento amplia ainda mais o escopo de proteção, regulamentando a conservação de dados

---

[27] A referida Diretiva é aplicável ao tratamento de dados pessoais no contexto da prestação de serviços de comunicações eletrônicas publicamente disponíveis nas redes públicas de comunicações pelos Estados membros.
[28] O *spam* refere-se àquelas mensagens comerciais não solicitadas.
[29] As *cookies* são pequenos ficheiros eletrônicos que se alojam no disco do computador quando o seu utilizador acessa a certos *websites*, e que recolhem e armazenam determinada informação pessoal sobre o utilizador como o nome, endereço eletrônico, *sites* visitados e buscas efetuadas, entre outros elementos. Geralmente, esta informação é posteriormente usada pela empresa que a recolhe para ações de publicidade dirigida (COUTO, 2006).

gerados ou tratados no contexto da oferta de serviços de comunicações eletrônicas publicamente disponíveis ou de redes públicas de comunicações.

A partir dos mesmos princípios que nortearam os documentos anteriores, a Diretiva 2006/24/CE inovou ao garantir a proteção do internauta quanto à retenção de seus dados. Segundo seus dispositivos, os dados pessoais do internauta poderão ser conservados desde que com fins investigativos ou para detecção e repressão de crimes graves, respeitando-se o que estivesse definido pela legislação interna de Estado-membro. Fixou-se que o armazenamento dos dados é por prazo limitado, não devendo exceder o período máximo de dois anos.

Esta legislação manteve-se vigente por mais de 15 anos, mas a dinamicidade do tema (especialmente por força da globalização dos fluxos informacionais e do surgimento e apropriação, por parte da população, de novas tecnologias) revelou inéditos problemas e desafios aos Estados membros, o que culminou na revisão das normativas. Assim, iniciou-se em 2009 um processo de atualização da legislação europeia por meio de consulta pública.

Essa iniciativa resultou na edição da Diretiva nº 136/2009, produzida com o objetivo de modernizar o sistema europeu de proteção de dados pessoais. Outro objetivo da nova normativa era reforçar os direitos dos cidadãos sobre seus dados pessoais, reduzindo as formalidades administrativas para sua utilização, medidas previstas no intuito de conferir mais clareza e coerência à normativa europeia (DEBATE, 2011).

Esse documento possui extrema relevância, pois estabelece diretrizes para uniformização do tratamento de proteção de dados pessoais pelos Estados-membros. Para tanto, prevê que o processamento de dados pessoais, no âmbito da União Europeia, deve ser feito de acordo com a legislação do respectivo Estado, a qual deve especificar as condições em que o processamento de dados é legal e prever as obrigações das entidades controladoras, o que deve ser feito conforme os princípios do processamento de dados pessoais impostos pela Diretiva (MORGADO, 2009).

Além disso, observa-se que foram feitas pequenas, mas importantes alterações em relação à Diretiva 58, de 2002. Primeiramente, ampliou-se a proteção estabelecida em seu art. 2°, passando a reconhecer como direito fundamental à confidencialidade[30] no tratamento de dados pessoais no setor das comunicações eletrônicas, ou seja, do desenvolvimento tecnológico emergiu uma nova categoria de direitos fundamentais. Por meio dessa nova

[30] Anteriormente o texto previa a harmonização das disposições dos Estados-Membros necessárias para garantir um nível equivalente de proteção dos direitos e liberdades fundamentais, abarcando como tal somente o direito à privacidade.

perspectiva, demonstra-se a importância de o legislador estar sempre atento à realidade social e cultural onde está inserido, tendo em vista o fato de que tanto a sociedade quando os direitos fundamentais são dinâmicos e devem acompanhar a evolução sociocultural instigada pelo fenômeno da globalização.

No campo conceitual, a Diretiva nº 136/2009 também apresentou avanços, pois o art. 2° precisou com maior clareza a "violação de dados pessoais," [31] considerando-se como tal as situações que envolvam destruição, perda, alteração ou uso de dados de maneira não autorizada pelo titular. E para assegurar que não ocorram situações que coloquem em risco os dados do usuário, o art. 4º determina que o prestador de serviço adote medidas no intuito de garantir a segurança no âmbito das comunicações eletrônicas, exigindo-se, inclusive, o consentimento prévio para que a empresa que atua no segmento possa tratar os dados do internauta pelo tempo necessário para a prestação do serviço ou realização da transação eletrônica.

Em contraste com a normativa anterior, esta nova Diretiva de 2009 altera (art. 13) o tratamento conferido aos *spams*, proibindo o envio de correio eletrônico para fins exclusivos de comercialização sempre que não houver endereço válido para o qual o destinatário possa enviar seu pedido para cessar a remessa. Essa, aliás, foi uma das mais significativas atualizações propostas pela nova Diretiva, pois garante que o usuário do serviço não seja alvo de invasões constantes e perturbadoras da sua intimidade e do seu sossego.

Da leitura dos termos da Diretiva de 2009 depreende-se que todo o esforço de aperfeiçoamento da legislação comunitária tem como objetivo acompanhar o desenvolvimento tecnológico, ofertando respostas e meios de enfrentamento que visam harmonizar as legislações nacionais e estabelecer um mínimo ético que deve ser observado para a proteção de dados de seus cidadãos.

O processo revisional iniciado no ano de 2009 também revela postura aberta e atenta dos Estados membros, que demostram compreender que a complexidade da sociedade em rede exige constante adequação legislativa. Tal postura é essencial em temas dinâmicos como os relacionados às inovações e usos das tecnologias informacionais, já que a normatização não pode ter a pretensão de perenidade e sim alicerçar-se sobre determinados princípios cuja abertura comporte interpretação e atualização constantes.

---

[31] "Violação de dados pessoais", uma violação da segurança que provoca, de modo acidental ou ilegal, a destruição, a perda, a alteração, a divulgação ou acesso não autorizado a dados pessoais transmitidos, armazenados ou de outro modo tratados no contexto da prestação de serviços de comunicações eletrônicas acessíveis ao público na Comunidade.

A vasta gama legislativa pertinente à proteção de dados pessoais, elaborada e adotada pela União Europeia, longe de sugerir confusão ou excesso legislativo, demonstra que os Estados Partes buscam aliar desenvolvimento tecnológico com proteção de direitos inerentes à pessoa. Esses esforços podem servir de exemplo para outros Estados que mais tardiamente se inserem na sociedade informacional, como o Brasil, que atualmente não possui legislação específica sobre o tema, registrando apenas Projeto de Lei de Proteção de Dados Pessoais, como se verá no próximo tópico.

3 A PROTEÇÃO DOS DADOS PESSOAIS NO BRASIL: desafios e perspectivas.

Quando o assunto é a proteção de dados pessoais, a situação mostra-se preocupante no Brasil, haja vista que a Constituição Federal não os contemplou como direitos fundamentais e tampouco existe legislação específica para a sua tutela, notadamente nos meios eletrônicos. Atualmente existem apenas regulamentações setoriais que não tratam de forma efetiva o problema exposto, o que coloca o país em posição de atraso legislativo se comparado até mesmo a outros países Latinos, a exemplo do Chile (Lei 19.628/99,), Argentina (Lei 25.326/2000 regulamentada pelo Decreto 1.558/2001), Uruguai (Lei nº 18.331/2008) e México (Ley Federal de Protección de Datos Personales em Posesión de los Particulares), que já dispõem de legislação própria (SILVA, 2011).

Muito embora existam problemas decorrentes do uso e tratamento de dados pessoais dos brasileiros, especialmente considerando o crescimento do número de internautas[32], observa-se que a proteção de dados ocorre de maneira indireta por meio da aplicação dos dispositivos constitucionais que tratam de direitos à privacidade e à intimidade. Não há, portanto, o reconhecimento expresso do *status* constitucional dos dados pessoais.

Do mesmo modo, a Carta Constitucional institui o Habeas Data[33], ação que permite ao indivíduo o conhecimento e a retificação de dados pessoais constantes de registros públicos ou banco de dados de entidades governamentais ou de caráter público (RABELO; GARCIA, 2011), outro remédio por vezes invocado por quem sofre violação em seus dados pessoais. No

[32] Conforme a última pesquisa IBOPE (2012) o número de pessoas com acesso à *Internet* em qualquer ambiente, (domicílios, trabalho, escolas, *lan houses* ou outros locais) chegou a 83,4 milhões no segundo trimestre de 2012. Esse número representou crescimento de 1% sobre os 82,4 do primeiro trimestre e de 7% sobre os 77,8 milhões do segundo trimestre do ano passado.

[33] Conforme assevera Kaminski (2010), o Habeas Data é um mecanismo de tutela à disposição do usuário de *Internet* que, vinculado a uma relação de consumo com um fornecedor, pretenda fazer valer seu direito de acessar os registros existentes em bancos de dados e em cadastros de consumo, bem como apagar informações errôneas, e complementar registros insuficientes ou incompletos.

entanto, levando-se em conta o fato de que na maioria das vezes as informações recolhidas ou manipuladas estão em bancos de dados privados, especialmente considerando-se o crescente uso da *Internet*, a efetividade desse instrumento torna-se limitada.

Analisando-se o ordenamento jurídico brasileiro percebe-se que ainda existem disposições que podem ser aplicadas ao tema e que se encontram no Direito do Consumidor, na legislação bancária e fiscal, bem como é possível alcançar tutela de alguns direitos de personalidade por meio de alguns dispositivos do Código Civil. Essas previsões se revelam limitadas, pois apenas garantem indenização em casos de danos já perpetrados, enquanto é sabido que a reparação é uma resposta tardia, que muitas vezes não satisfaz a vítima. Portanto, não há uma opção pelo tratamento autônomo dos dados pessoais lançados no ciberespaço, tampouco existindo um conjunto articulado de medidas jurídicas preventivas que atendam aos desafios descortinados pela crescente utilização das tecnologias da informação e comunicação.

Para tentar responder adequadamente à nova realidade que emerge da inserção dos brasileiros na sociedade informacional, em 29 de outubro de 2009 foi lançado projeto para a construção colaborativa de um Marco Civil da *Internet* no país[34], o que foi feito por meio de medida conjunta da Secretaria de Assuntos Legislativos da Justiça (SAL/MJ) e da Escola de Direito da Fundação Getúlio Vargas. A elaboração de um marco civil visou articular um conjunto de normas que garantissem direitos aos internautas, provedores e ao próprio governo. Na data foi apresentado o texto-base produzido pelo Ministério da Justiça, que identificou e propôs a sistematização dos principais temas referentes à *Internet* que se encontravam (e se encontram) pendentes de regulação no país (MARCO CIVIL DA *INTERNET*, 2012).

No mesmo intuito, porém com um viés voltado especificamente à proteção de dados pessoais, em 30 de novembro de 2010, a Secretaria de Assuntos Legislativos e o Departamento de Proteção e Defesa do Consumidor do Ministério da Justiça (DPDC) lançaram um debate público sobre privacidade e proteção de dados pessoais. Essa iniciativa contou com apoio e parceria de importantes instituições, dentre elas o Observatório Brasileiro de Políticas Digitais do Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas, do

[34] A votação do Projeto de Lei, enviado ao Congresso sob o número 2.126/2011, estava marcada para dia19 de setembro de 2012, na Câmara dos Deputados. Entretanto, foi adiada, tendo em vista o baixo número de parlamentares no período que antecede as eleições municipais, conforme salientou o relator da comissão especial e deputado federal Alessandro Molon (PT-RJ) (FREIRE, 2012).

Rio de Janeiro, articuladas com o objetivo de elaborar um anteprojeto de lei sobre a proteção de dados na *Internet* (MINISTÉRIO DA JUSTIÇA, 2012).

Ressalta-se que dentre os principais objetivos do projeto está o de definir a proteção da privacidade, as possíveis formas de acesso, a divulgação e a circulação de informações dos cidadãos (MENDES, 2012). Esse projeto mostra-se de grande importância para o internauta brasileiro, pois além da tutela dos seus dados pessoais, considerados como bem jurídico autônomo, ainda reconhece o direito de autodeterminação, segundo o qual o usuário tem o poder de decidir quem poderá fazer uso de seus dados e em que condições, estando legitimado ainda a cancelar as autorizações de tratamento de suas informações pessoais.

Os atores (pessoas físicas e instituições) envolvidos nesse processo de construção democrática e coletiva propuseram que o debate fosse realizado através de um *blog* que ficaria online por sessenta dias[35].

Com essa estratégia objetivou-se a interação da sociedade civil, empresas do segmento, instituições, centros de pesquisa e representantes governamentais, na tentativa de garantir voz e oportunidade de participação a todos os interessados no tema. Esse processo de construção coletiva ancorou-se em princípios republicanos, sobretudo porque privilegiou a discussão democrática, com a participação e coordenação de ideias.

Desse intenso debate público acerca da privacidade e proteção de dados pessoais no Brasil resultou o projeto de Lei protocolado no Congresso Nacional sob o número 4.060/2012. Contudo, ao cotejar a proposta inicial com o texto consolidado e enviado ao parlamento, constata-se que houve substanciais modificações.

Conforme se pode observar, inicialmente o Projeto nº 4.060/2012 destaca seu objetivo primeiro, isto é, garantir e proteger, no âmbito do tratamento de dados pessoais, a dignidade e os direitos fundamentais da pessoa natural, particularmente em relação a sua liberdade, privacidade, intimidade, honra e imagem[36]. Assim, deve-se promover a proteção de tais direitos com observância dos princípios constitucionais da defesa do consumidor, livre iniciativa, liberdade de comunicação e ordem econômica, nos termos dos artigos 1º, IV, 5º, inc. IX, XXXII, 170 e 220 da Constituição Federal.

O projeto de lei brasileiro preocupou-se em oferecer a definição conceitual do bem jurídico a que visa tutelar. Para tanto, o 7° define dados pessoais como quaisquer informações

---

[35] A previsão inicial foi alterada e o blog foi mantido por mais 30 (trinta) dias, até o final do mês de abril de 2011.

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

que permitam a identificação exata e precisa de uma pessoa determinada. Contrastando-se esse conceito com aquele oferecido pela Diretiva 46 do Parlamento Europeu, nota-se que no caso brasileiro o escopo da proteção é mais restrito, haja vista que a normativa europeia considera dados pessoais qualquer informação relativa a uma pessoa singular identificada ou *identificável*, de forma direta ou indireta.

Assim, conforme a definição brasileira, um provedor está autorizado a coletar esparsas informações referentes a uma mesma pessoa sem que esse conjunto de informações seja considerado dado pessoal. Com essa disposição parece que o Projeto brasileiro ignora o fato de que a reunião de diversas informações sobre a pessoa poderá torná-la identificável e, portanto, vulnerável no ambiente virtual, especialmente considerando a falta de qualquer controle sobre esses fluxos informacionais.

No Capítulo II o Projeto abarca os requisitos para tratamento de dados pessoais, apresentando princípios básicos a serem observados, tais como o princípio da lealdade e boa fé[37], aplicáveis sempre no intuito de atender aos legítimos interesses dos titulares dos dados. Além disso, há importante previsão no sentido de que os responsáveis pelo tratamento de dados e seus eventuais subcontratados adotem medidas tecnológicas atuais e específicas a fim de reduzir o risco de destruição, perda, acesso não autorizado ou de tratamento não permitido pelo titular, especialmente no caso dos dados sensíveis. Esta medida se mostra importante, pois forçará as empresas que atuam no setor a buscar o aprimoramento técnico contínuo, no intuito de oferecer as melhores tecnologias para minimizar os riscos inerentes à atividade. Além disso, como a empresa é responsável pelo armazenamento, tratamento e/ou sigilo de importantes informações, exige-se maior atenção e cuidado do prestador de serviço.

Salienta-se que o Projeto de Lei assegura proteção especial para os dados sensíveis, permitindo seu recolhimento e tratamento somente quando solicitado/autorizado pelo titular. À revelia do titular os dados dessa natureza somente poderão ser recolhidos e tratados mediante imposição legal.

---

[37] Conforme lições de uma das principais responsáveis pela discussão do instituto da boa-fé no ordenamento brasileiro, Judith Martins Costa (1999, p. 411.), boa-fé seria um modelo de conduta social, arquétipo ou *standard jurídico*, segundo o qual cada pessoa deve ajustar a própria conduta a esse arquétipo, obrando como obraria um homem reto: com honestidade, lealdade e probidade. Do mesmo modo, Rosenvald (2005, p. 116) assevera que o dever de lealdade está intimamente ligado com a ética e a honestidade no trato entre as pessoas. É uma medida de cooperação recíproca que impõe às partes a abstenção sobre qualquer conduta capaz de falsear o objetivo do negócio ou desequilibrar o jogo das prestações por elas consignado. Agir com deslealdade implica atingir a dignidade do outro contratante. Desta forma, no que se refere ao tratamento de dados pessoais, cabe aos responsáveis agir de forma honesta e proba, isto é, pautando-se pela ética e honestidade no tratamento das informações que lhes são passadas, tendo em vista seu acesso aos dados pessoais do internauta, bem como o tratamento e armazenamento dessas informações. Os responsáveis terão, portanto, a obrigação de tratar os dados da melhor forma possível, garantindo-se o sigilo e proteção dos dados transmitidos pelo titular.

Da mesma forma, apresenta-se relevante o fato de que é assegurado ao titular a possibilidade de bloquear o registro de seus dados pessoais constante nos bancos de dados informatizados, exceto se necessário para cumprimento de obrigação legal ou contratual.

Como se vê, o projeto de lei em análise contempla o reconhecimento de um novo direito, isto é, o direito de autodeterminação das informações e dados pessoais prestados ou coletados por qualquer meio. Esta previsão, se efetivamente incorporada ao ordenamento jurídico brasileiro, será de suma importância, pois além de inaugurar o processo de regulamentação do tratamento de dados pessoais, reconhece no campo normativo o direito de o internauta controlar "como" e "quando" suas informações serão utilizadas, decidindo quem terá acesso a seus dados pessoais e como eles serão armazenados.

É preciso advertir, no entanto, que o simples reconhecimento normativo do direito à autodeterminação informativa não terá o condão de alterar a realidade se esse dispositivo não estiver acompanhado de outras medidas políticas e da mudança de postura por parte de tomadores e fornecedores de serviços *online*. Com efeito, sabe-se que na prática o direito à autodeterminação informativa poderá se revelar de duvidosa efetividade, pois ao bloquear o registro o usuário não poderá mais usufruir dos serviços oferecidos por aquele prestador.

No que se refere ao tratamento dos chamados *spams*, o parágrafo único do art. 15 autoriza o seu envio, salvo se o titular solicitar o bloqueio do tratamento dos seus dados ou tiver manifestado expressamente ao emissor do *e-mail* o interesse em não mais recebê-los. Ora, por este dispositivo percebe-se que a regra passa a ser o envio dos *spams* por parte do fornecedor, o que só cessa com a recusa por parte do consumidor, privilegiando-se os interesses econômicos em detrimento do direito ao sossego e à intimidade do usuário dos serviços. Essa opção legislativa é no mínimo questionável, sobretudo se for considerada a tábua axiológica que alicerça a Carta Constitucional de 1988.

Mas o que suscita crítica ainda mais contundente é que o documento em análise ainda autoriza os responsáveis pelo tratamento de dados a compartilhá-los com empresas integrantes de um mesmo grupo econômico, parceiros comerciais ou terceiros que direta ou indiretamente contribuam para a realização do tratamento de dados pessoais (desconhecidos do titular das informações), desde que respeitados os princípios da boa fé e da lealdade.

Ora, permitir esse tipo de comportamento por parte do fornecedor de serviços evidencia por si só um claro desrespeito ao princípio da boa-fé, um dos pilares do Código de Defesa do Consumidor, igualmente contemplado no art. 422, do Código Civil de 2002. Esse princípio tem forte inspiração social e desdobra-se em deveres de conduta, dentre eles o dever de informação, segundo o qual o provedor tem que informar ao internauta quem acessa e

utiliza suas informações. Logo, o art. 15 do Projeto de Lei viola esse princípio, já que permite o repasse de dados a empresas desconhecidas do internauta, o que aumenta a sua vulnerabilidade e afronta o Código de Defesa do Consumidor.

No que tange ao tratamento de dados pessoais de crianças, o art. 17 somente autoriza o seu recolhimento mediante o consentimento dos pais, responsáveis ou por imposição legal, privilegiando o princípio da Proteção Integral[38], de matriz constitucional (art. 227, da CF/88), inspirador da Lei 8.069, de 1990. Quanto a essas previsões o Projeto de Proteção de Dados Pessoais encontra-se adequado, eis que se coaduna com a orientação constitucional de proteger de maneira especial aqueles cujo desenvolvimento ainda é incompleto.

Em relação à tutela fiscalizatória e sancionatória observa-se que o projeto em tela não contemplou medidas específicas, limitando-se a mencionar que os responsáveis pelo tratamento de dados pessoais que incorrerem nas infrações legais ficarão sujeitos à aplicação das sanções elencadas no Código de Defesa do Consumidor[39]. Nesses casos é possível a celebração de Compromissos de Ajustamento de Conduta (CAC), a serem firmados entre representantes dos órgãos e entidades de proteção consumerista, de um lado e, de outro, por empresas e responsáveis que incorrerem nas condutas violadoras de dados pessoais.

A opção por essa alternativa de solução de conflitos se mostra adequada, sobretudo porque o objetivo precípuo da futura lei de proteção de dados pessoais não deve ser punitivo, prevalecendo o caráter preventivo e pedagógico. Ao firmar o CAC oportuniza-se que os fornecedores de serviços e produtos que atuam na *web* adotem novas posturas, o que a médio

---

[38] A partir da adoção da Doutrina da Proteção Integral no Ordenamento Jurídico brasileiro, passa-se a reconhecer na criança e no adolescente um sujeito pleno de direitos que, por estar em uma peculiar condição de desenvolvimento, precisa de ampla proteção e prioridade. Por meio deste novo paradigma, o centro da proteção passa da sociedade para a população infanto-juvenil, que torna-se merecedora de cuidados e atenção de todos os atores sociais (SILVA, 2009).

[39] Neste caso, podem ser aplicadas as sanções administrativas previstas no art. 56, bem como as sanções decorrentes de infrações penais, conforme previsto nos arts. 72 e 73:

- Art. 56. As infrações das normas de defesa do consumidor ficam sujeitas, conforme o caso, às seguintes sanções administrativas, sem prejuízo das de natureza civil, penal e das definidas em normas específicas:

I - multa; II - apreensão do produto; III - inutilização do produto; IV - cassação do registro do produto junto ao órgão competente; V - proibição de fabricação do produto; VI - suspensão de fornecimento de produtos ou serviço; VII - suspensão temporária de atividade; VIII - revogação de concessão ou permissão de uso; IX - cassação de licença do estabelecimento ou de atividade; X - interdição, total ou parcial, de estabelecimento, de obra ou de atividade; XI - intervenção administrativa; XII - imposição de contrapropaganda.

Parágrafo único. As sanções previstas neste artigo serão aplicadas pela autoridade administrativa, no âmbito de sua atribuição, podendo ser aplicadas cumulativamente, inclusive por medida cautelar, antecedente ou incidente de procedimento administrativo.

- Art. 72. Impedir ou dificultar o acesso do consumidor às informações que sobre ele constem em cadastros, banco de dados, fichas e registros:

Pena Detenção de seis meses a um ano ou multa.

- Art. 73. Deixar de corrigir imediatamente informação sobre consumidor constante de cadastro, banco de dados, fichas ou registros que sabe ou deveria saber ser inexata:

Pena Detenção de um a seis meses ou multa.

e longo prazo pode se revelar mais eficaz do que o mero papel simbólico representado pela sanção, típica do Direito Penal.

Outro destaque fica por conta da previsão de que as entidades representativas de responsáveis pelo tratamento de dados pessoais possam instituir Conselhos de Autorregulamentação, encarregados de elaborar códigos definidores de parâmetros éticos para tratamento de dados e comunicação comercial, bem como determinar as condições para sua organização, funcionamento, controle e sanções. A composição de conselhos dessa natureza visa a dar um mínimo de alinhamento à ação das empresas que atuam no segmento evitando, inclusive, situações de concorrência desleal entre aquelas que respeitam os dados pessoais dos consumidores e outras que porventura atuem em desrespeito à lei.

Se a harmonização da atuação do setor responsável pelo recolhimento e tratamento de dados pela via da autorregulação pode ser suficiente entre as empresas, não se pode apostar que todos os conflitos possam ser resolvidos pela autorregulação. Analisando-se os termos do Projeto de Lei em tramitação e contrastando seu texto com as sugestões ofertadas na fase de discussão, percebe-se que houve a supressão do art. 39 do antigo texto que, a exemplo das normativas europeias, contemplava a criação de uma Autoridade Nacional Regulamentadora, encarregada de fiscalizar e aplicar sanções administrativas às empresas que desrespeitassem dados pessoais dos usuários.

A proposta em tramitação é merecedora de contundentes críticas quanto a essa supressão, que fragiliza ainda mais os direitos do titular dos dados. Ao excluir a atuação de uma autoridade regulamentadora privilegiou-se mais uma vez interesses econômicos e a liberdade do fornecedor, em detrimento da proteção do consumidor.

Outra triste constatação é que esta atual versão enviada ao Congresso Nacional desconsidera a riqueza das discussões anteriores e da participação democrática, optando pela simplificação e pela valorização da liberdade dos provedores, na medida em que foram previstos apenas instrumentos como Compromissos de Ajustamento de Conduta e autorregulamentação, ambos favoráveis aos seus interesses. Essas medidas mostram-se meramente paliativas, tendo em vista o óbvio, isto é, os prestadores de serviço não criarão medidas desfavoráveis ao exercício de sua atividade. A autorregulamentação, por seu turno, embora possa ser útil na relação entre fornecedores, não se mostra medida totalmente eficaz na proteção do *consumidor*, haja vista que essa espécie de regulação pressupõe atores em condições de estabelecerem de comum acordo as normas de conduta aplicáveis, o que inexiste entre consumidor e fornecedor que atuam no ambiente virtual.

CONSIDERAÇÕES FINAIS

O desenvolvimento das tecnologias da informação e comunicação imprimiu um novo ritmo à sociedade, tornando porosas as fronteiras, instantaneamente ultrapassadas pelos fluxos informacionais. Em meio a notícias, publicidades, apelos ao consumo, comunicações e interações que povoam o ambiente virtual, cotidianamente são disponibilizadas informações pessoais bastante reveladoras sobre os internautas, sobressaindo-se aquelas que tomam a forma de dados pessoais, objeto de análise neste artigo.

Como exposto ao longo do texto, a partir de um conjunto de informações disponibilizadas (voluntariamente ou involuntariamente) pelo internauta é possível identificar uma pessoa, determinar seus hábitos de consumo e suas preferências, publicizando para terceiros determinados dados pessoais que só interessam ao seu titular. Uma vez lançados no ambiente virtual, seu destino escapa ao controle do internauta, que não dispõe de meios de impedir seu armazenamento e repasse a outros, distintos de quem originariamente os recolheu. Essa perda crescente da autodeterminação informativa é uma das faces da sociedade informacional, o que desafia a comunidade jurídica a refletir sobre determinados problemas atuais, sobretudo nos Estados em que a inclusão digital foi mais tardia, como no caso brasileiro.

O enfrentamento deste tema, ainda novo e permeado de complexidades, não comporta respostas simples e lineares, como aquelas ofertadas pelo Direito construído na modernidade. Para além disso, as soluções exigem a análise do fenômeno em toda a sua inteireza, reconhecendo que na *web* se realizam as mais variadas interações e transações, sendo que em alguns casos o internauta até tem mais condições de escolher entre divulgar ou não determinadas informações pessoais; enquanto em outras situações essas informações são coletadas, tratadas e transmitidas para terceiros sem que o seu titular tenha qualquer controle sobre o processo. Em qualquer caso, o oferecimento de dados pessoais é condição necessária para a inclusão digital dessa pessoa, pois para acessar a *Internet* terá que prestar determinadas informações a um provedor de acesso, o que já é suficiente para perder o controle sobre o que foi informado.

Considerando o crescimento do número de brasileiros conectados à *Internet*, as características da *web*, que ampliam a liberdade dos particulares e das empresas para capturar, armazenar e transmitir informações e a ausência de lei específica sobre o tema no Brasil buscou-se, neste trabalho, lançar um olhar sobre a experiência já desenvolvida nos Estados há

mais tempo inseridos na sociedade informacional, o que determinou o exame das normativas da União Europeia.

O tratamento jurídico do tema conferido pelos Estados Partes evidencia que é possível adotar um mínimo de regulação para a captura e tratamento de dados pessoais no ciberespaço, o que demonstra que apesar de o ambiente virtual se constituir em espaço privilegiado para exercer a liberdade de informação e comunicação e da crença na cultura libertária da *Internet*, que não combinaria com normas estatais rígidas, é desejável e necessário um mínimo de regulação. Ao afirmar a necessidade de um mínimo de regulação não se está a defender apenas a existência de leis penais para sancionar quem se apropria indevidamente e utiliza dados pessoais sem autorização de seu titular. Tampouco se está a advogar que o Estado regulamente isoladamente a matéria por meio de um modelo de regulação estatal rígido, nos moldes das vetustas legislações *oitocentistas*.

O primeiro e importante passo seria reconhecer os dados pessoais e o direito à autodeterminação informativa como direitos fundamentais e, a partir daí, empoderar os atores sociais, sobretudo o cidadão, para impedir ou fazer cessar as violações aos seus dados, assegurando-se tratamento digno aos internautas, como preceitua a Carta Constitucional. Para atingir esse grau de tutela poderia ser observado o exemplo de regulação adotado na União Europeia.

Conforme exposto neste artigo, os Estados europeus desde a década de oitenta normatizam a matéria a partir de sucessivas Diretivas, aperfeiçoadas sempre que o desenvolvimento tecnológico impôs novos ritmos às interações sociais e às transações econômicas. Essa abertura, garantida pela adoção de princípios (lealdade, respeito à finalidade do recolhimento aos dados, proporcionalidade) e as constantes revisões empreendidas permitem que a legislação não se cristalize e se mantenha em constante sintonia com os usuários. Como se percebe, o foco de proteção é a pessoa, e não meramente os interesses econômicos.

Ademais, além de enunciar direitos para o titular dos dados pessoais, a União Europeia tratou de oferecer mecanismos para a sua efetivação, prevendo a criação de uma Autoridade de Garantia, capaz de fiscalizar o cumprimento das medidas previstas. Apostou na atuação na seara administrativa, que também oferece espaço para a composição dos interesses contrapostos, evitando a judicialização dos conflitos.

Enquanto os Estados europeus há aproximadamente vinte anos procuram caminhos e melhores estratégias para regular a matéria, o Brasil, por sua vez, protela e chega a apresentar retrocessos.

Com efeito, enquanto o anteprojeto apresentado pelo Ministério da Justiça à sociedade civil brasileira possuía um texto muito semelhante às previsões da União Europeia, que registra vários mecanismos de proteção aos dados pessoais, o Projeto de Lei nº 4.060/2012 enviado ao Congresso Nacional sofreu drásticas alterações, desfigurando-se. Ao sofrer supressão em vários de seus mecanismos de proteção ao usuário da *Internet* acaba desviando-se de sua finalidade precípua de garantir a melhor proteção e amparo ao titular dos dados pessoais que interage na *Internet*.

O novo Projeto de Lei encaminhado ao Congresso Nacional revela que o Brasil afasta-se da proposta de regulação de dados pessoais construída coletivamente e retrocede no tratamento do tema. O texto ora em tramitação dissocia-se tanto dos princípios extraídos das normativas europeias, que claramente tinham inspirado os debates que culminaram na proposta inicial (hoje superada), quanto dos princípios da boa-fé objetiva e do dever de informação, baluartes do Código de Defesa do Consumidor, atualmente também contemplados no Código Civil Brasileiro.

A supressão e a modificação de inúmeros dispositivos que garantiam a maior proteção do internauta brasileiro e a consequente ampliação da liberdade dos prestadores de serviços na *Internet* aprofunda a desigualdade já inerente a essa relação jurídica, ampliando a vulnerabilidade do titular de dados. Os pontos críticos vão desde a previsão de tratamento restritivo na conceituação de dados pessoais, o que torna o titular vulnerável a *sites* que criam perfis de consumo ao combinarem informações pessoais para, posteriormente, alvejar de *spams* o internauta; até o notório privilégio concedido aos fornecedores de serviços que atuam no segmento, que podem transferir os dados do seu cliente para terceiros, cuja identidade seja ignorada pelo internauta.

Quanto aos mecanismos de efetivação da proteção, o Projeto de Lei nº 4.060/2012 também se mostra insuficiente e se distancia da tutela perseguida na União Europeia. Conforme destacado, a proposta anterior contemplava a criação de uma Autoridade Nacional Regulamentadora, com competência para fiscalizar a aplicação da lei e aplicar sanções administrativas àquelas empresas que a descumprissem, o que foi suprimido no projeto atual. Há apenas a previsão de celebração de Compromissos de Ajustamento de Conduta (CAC) com responsáveis que incorrerem em infração às normas prevista no Projeto de Lei, bem como a possibilidade de as entidades representativas de responsáveis pelo tratamento de dados pessoais instituírem Conselhos de Autorregulamentação. Todavia, conforme frisado ao longo do artigo, essa previsão também não se revela uma alternativa em defesa do consumidor, pois para a autorregulação ocorrer é preciso que os sujeitos da relação

(fornecedores e usuários) estabeleçam as regras de uso de comum acordo, pressupondo igualdade de condições no diálogo, o que não se verifica na prática.

Ao revelar o desenho da futura legislação brasileira de proteção de dados pessoais e as escolhas ideológicas sobre as quais está alicerçada, resta evidente que ainda há muito que avançar no Brasil, sobretudo se comparado com as normativas europeias. Como se depreende do que ficou demostrado na seção 2 deste artigo, enquanto na União Europeia as normativas e Diretivas tem clara inspiração social, a seção 3 ratificou a desconfiança inicial que inspirou a problematização deste artigo: em *terra brasilis* ainda sopram os ventos do liberalismo econômico que se sobrepõe à proteção da dignidade da pessoa, tornando o Projeto de Lei nº 4.060/2012 insuficiente para efetivamente tutelar os dados pessoais dos internautas brasileiros, o que por certo também é um obstáculo para a efetividade dos objetivos da República Federativa do Brasil.

REFERÊNCIAS

AGÊNCIA BRASIL - Empresa Brasil de comunicação. **Aprovação de projetos sobre tipificação de crimes cibernéticos divide especialistas**. Disponível em: < http://agenciabrasil.ebc.com.br/noticia/2012-11-08/aprovacao-de-projetos-sobre-tipificacao-de-crimes-ciberneticos-divide-especialistas> Acesso em: 01 nov. 2012.

ALMEIDA NETO, Honor de. **Trabalho infantil na terceira revolução industrial**. Disponível em: <http://www.pucrs.br/edipucrs/online/trabalhoinfantil/trabalhoinfantil/2.1.1.html> Acesso em: 23 ago. 2012.

CASELLA, Paulo Borba. **Comunidade Européia e seu Ordenamento Jurídico**. São Paulo: LTr, 1994.

CASTELLS, Manuel. **A sociedade em rede**. 11. ed. Traduzido por Roneide Venâncio Majer. São Paulo: Paz e Terra, 2008. v. 1.

CASTRO, Catarina Sarmento e. **Direito da informática, privacidade e dados pessoais**. Coimbra: Edições Almedina, 2005.

CGI.BR apresenta **TIC Domicílios 2011**. Disponível em: http://www.s2publicom.com.br/imprensa/ReleaseTextoS2Publicom.aspx?press_release_id=27055> Acesso em: 10 mai. 2012.

_____: **por uma Internet brasileira cada vez melhor.** Disponível em: <http://www.cgi.br/br.htm> acesso em: 22 ago. 2012.

CETIC.BR. **Sobre o CETIC. BR. 2005**. Disponível em: < http://www.cetic.br/sobre-ceticbr/> Acesso em: 18 de mai. 2012.

COELHO, Camila. **O direito e as novas tecnologias da informação e comunicação**. Disponível em: <http://www.cgi.br/br.htm> acesso em: 25 ago. 2012.

COMM, Joel. **O poder do Twitter***:* estratérias para dominar seu mercado e atingir seus objetivos com um *tweet* por vez. São Paulo: Editora Genta, 2009.

COSTA, Judith Martins. **A boa-fé no direito privado**. São Paulo: RT, 1999.

COSTA, Paulo Tarso da. **Princípio da igualdade**. Disponível em: <http://abadireitoconstitucional.blogspot.com.br/2009/12/principio-da-igualdade.html> Acesso em: 24 ago. 2012.

COUTO, Margarida. **Privacidade e Tecnologias Digitais***:* visão europeia. Disponível em: <http://www.abdi.org.br/visualizarImpressao.cfm?COD=8&X=16> Acesso em: 27 set. 2012

DEBATE DADOS PESSOIAS. **Contexto Internacional**. Disponível em: <http://culturadigital.br/dadospessoais/contexto-internacional/> Acesso em: 08 nov. 2012.

DE LA CUEVA, Pablo Lucas Murillo. **Informática y protección de datos personales**. Madri: Centro de Estudios Constitucionales, 1993.

FERREIRA FILHO, Manoel Gonçalves. **Direitos humanos fundamentais**. São Paulo: Saraiva, 1999.

FREIRE, Raquel. **Votação do Marco Civil da Internet é adiada para outubro**. Disponível em: < http://www.techtudo.com.br/noticias/noticia/2012/09/votacao-do-marco-civil-da-*Internet*-e-adiada-para-outubro.html> Acesso em: 15 out 2012.

GONCALVES, Maria Eduarda. **Direito da informação***:* novos direitos e formas de regulação na sociedade da informação. Coimbra: Almedina, 2003.

IBOPE. **Número de brasileiros com acesso à Internet chega a 83,4 milhões de pessoas**. Disponível em: <http://www.ibope.com.br/pt-br/noticias/Paginas/Numero-de-brasileiros-com-acesso-a-*Internet*-chega-a-83-milhoes-de-pessoas.aspx> Acesso em: 15 out 2012.

KAMINSKI, Omar. **O direito à privacidade e proteção aos dados pessoais no Brasil**. Rio de Janeiro, D.P.D.C.; U.E.R.G, 11 ago. 2010. Seminário sobre Proteção à Privacidade e aos Dados Pessoais no Brasil. Entrevista concedida a Marcel Leonardi. Disponível em: <http://www.zappiens.br/portal/VisualizarVideo.do?_InstanceIdentifier=0&_EntityIdentifier=cgiMyo1DZCLVIWgqd1sNXRMLjZF_8FYwlqnyjIURbcCZlM.&idRepositorio=0 > Acesso em: 15 out. 2012.

LIMBERGER, Têmis. Da evolução do Direito a ser deixado em paz à proteção dos dados pessoais. **Revista Novos Estudos Jurídicos**. Vol. 14, n° 2, p. 27-53, 2° quadrimestre 2009.

MARCO CIVIL NA *INTERNET*. **Sobre.** Disponível em: <http://culturadigital.br/marcocivil/sobre/> Acesso em: 19 set 2012.

MATTELART Armand. **História da sociedade da informação**. Traduzido por Nicolás Nyími Campanário. São Paulo: Loyola , 2002.

MENDES, Vannildo. **Governo abre debate sobre proteção de dados pessoais**. Disponível em: <http://www.istoedinheiro.com.br/noticias/42676_GOVERNO+ABRE+DEBATE+SOBRE+PROTECAO+DE+DADOS+PESSOAIS> Acesso em: 25 out. 2012.

MINISTÉRIO DA JUSTIÇA lança debate sobre projeto de proteção a dados pessoais. **Portal do Ministério da Justiça**. Disponível em: <http://portal.mj.gov.br/data/Pages/MJB1F03491ITEMIDEA899C9657584C408AF72867D6D8A17EPTBRIE.htm> Acesso em: 25 out. 2012.

MORGADO, Laerte Ferreira. O cenário internacional de proteção de dados pessoais. Necessitamos de um Código Brasileiro? In: **Âmbito Jurídico**, Rio Grande, XII, n. 65, jun 2009. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=6336>. Acesso em: 18 mai. 2012.

PEREIRA, Marcelo Cardoso. **Direito à intimidade na Internet**. Curitiba: Juruá, 2005.

_____. **Direito à intimidade na Internet**. Curitiba: Juruá, 2006.

PÉREZ LUÑO, Antonio-Enrique. **Derechos humanos, Estado de Derecho y Constitución**. 9. ed. Madri: Editorial Tecnos, 2005.

_____. Internet y los derechos humanos. In: **Anuario de Derechos Humanos**. Nueva Época. Vol. 12. 2011, p. 287-329. Disponível em:< http://revistas.ucm.es/index.php/ANDH/article/view/38107>. Acesso em: 08 mar 2013.

PESQUISA sobre o uso das tecnologias de informação e comunicação no Brasil: **TIC Domicílios e TIC Empresas 2011** = Survey on the use of information and communication technologies in Brazil : ICT Households and Enterprises 20111/[coordenação executiva e editorial/ executive and editorial coordination,Alexandre F. Barbosa ; tradução /translation Karen Brito Sexton (org.)]. – São Paulo: Comitê Gestor da *Internet* no Brasil, 2012.

RABELO, Iglesias Fernanda de Azevedo; GARCIA, Filipe Rodrigues. **O direito à autodeterminação informativa**. Disponível em: < http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=10473&revista_caderno=7> Acesso em: 08 nov. 2012.

RECUERO. Raquel. **Redes sociais na Internet**. Porto Alegre: Sulina, 2009.

REINALDO FILHO, Demócrito. **Comissão europeia aprova novos modelos de cláusulas contratuais para a transmissão de dados pessoais a países não membros da EU.** Disponível em: < http://www.boletimjuridico.com.br/doutrina/texto.asp?id=565 >. Acesso em: 29 set. 2012.

ROSENVALD, Nelson. **Dignidade humana e boa-fé no código civil**. São Paulo: Saraiva, 2005.

ROVER, Aires. A democracia digital possível. **Revista Sequência**, nº 52, p. 85-104, jul. 2006. Disponível em: <http://periodicos.ufsc.br/index.php/sequencia/article/view/15202/13827>. Acesso em: 15 março 2012.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 33º ed. São Paulo: Malheiros, 2009.

SILVA, Letícia Brum da. A sociedade informacional e a proteção jurídica de dados pessoais no Brasil. In*:* XX Congresso Nacional do CONPEDI, 2011, Belo Horizonte. **Anais.** Florianópolis: Fundação Boiteux, 2012.

TAKAHASHI, Eduardo Tadao. *Brasil: RNP* – **Conselho Nacional de Desenvolvimento Científico e Tecnológico.** Disponível em: <http://interred.wordpress.com/1989/11/02/brasil-rnp-conselho-nacional-de-desenvolvimento-cientifico-e-tecnologico > acesso em: 22 ago. 2012.

UNIÃO EUROPEIA. Comissão Europeia. **Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados** (regulamento geral sobre a proteção de dados). Disponível em:<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:PT:PDF> Acesso em: 01 nov. 2012.

_____. Parlamento Europeu e do Conselho. **Directiva 95/46/CE**, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:pt:HTML>. Acesso em: 06 jan. 2013.

_____. Parlamento Europeu e do Conselho. **Directiva 97/66/CE**, de 15 de Dezembro de 1997, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das telecomunicações. Disponível em: < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0066:PT:HTML>. Acesso em 12 dez. 2012.

_____. Parlamento Europeu e do Conselho. **Regulamento (CE) n.° 45/2001 do Parlamento Europeu e do Conselho**, de 18 de Dezembro de 2000, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados. Disponível em: < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001R0045:pt:HTML>. Acesso em: 12 dez. 2012.

_____. Parlamento Europeu e do Conselho. **Directiva 2002/58/CE** , de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas. Disponível em: < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:PT:HTML>. Acesso em: 14 dez. 2012.

_____. Parlamento Europeu e do Conselho. **Directiva 2006/24/CE**, de 15 de Março de 2006 , relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva 2002/58/CE. Disponível em: < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:PT:HTML>. Acesso em: 14 dez. 2012.

_____. Parlamento Europeu e do Conselho. **Directiva 2009/136/CE**, de 25 de Novembro de 2009. Disponível em: < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:01:PT:HTML>. Acesso em: 19 dez. 2012.

_____. Parlamento Europeu e do Conselho. **Directiva 2000/31/CE** , de 8 de Junho de 2000 relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico, no mercado interno («Directiva sobre o comércio electrónico»). Disponível em:< http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:Pt:HTML>. Acesso em: 19 dez. 2012.

_____. **Os Fundadores da EU**. Disponível em: < http://europa.eu/about-eu/eu-history/founding-fathers/index_pt.htm>. Acesso em: 14 ago 2012.