UNIVERSIDADE FEDERAL DE JUIZ DE FORA
FACULDADE DE DIREITO
ALEXANDRE RIBEIRO DA SILVA

A PROTEÇÃO DE DADOS NO BRASIL: a tutela do direito à privacidade na sociedade de informação

Juiz de Fora – MG
2017

ALEXANDRE RIBEIRO DA SILVA

A PROTEÇÃO DE DADOS NO BRASIL: a tutela do direito à privacidade na sociedade de informação

Dissertação apresentada ao Programa de Pós-Graduação *Stricto Sensu* da Faculdade de Direito da Universidade Federal de Juiz de Fora como requisito para a obtenção do título de mestre na área de concentração Direito e Inovação, sob a orientação do Professor Doutor Sérgio Marcos Carvalho de Ávila Negri.

Juiz de Fora – MG

2017

ALEXANDRE RIBEIRO DA SILVA

A PROTEÇÃO DE DADOS NO BRASIL: a tutela do direito à privacidade na sociedade de informação

Dissertação apresentada ao Programa de Pós-Graduação *Stricto Sensu* da Faculdade de Direito da Universidade Federal de Juiz de Fora como requisito para a obtenção do título de mestre na área de concentração Direito e Inovação, sob a orientação do Professor Doutor Sérgio Marcos Carvalho de Ávila Negri.

Aprovada em de de

BANCA EXAMINADORA

_____

Universidade Federal de Juiz de Fora (UFJF)

_____

Universidade Federal de Juiz de Fora (UFJF)

_____

DEDICATÓRIA

Dedico este estudo à Mariana, minha companheira do mestrado e da vida.

AGRADECIMENTOS

Agradeço aos meus pais Nelson Geraldo Nogueira da Silva e Ângela Maria Ribeiro da Silva, por me ensinarem o valor do esforço e da honestidade na construção de meus sonhos.

À minha companheira Mariana Colucci Goulart Martins Ferreira por todas as horas de estudos conjuntos. Pelos Seminários, Congressos e auxílio durante todo o mestrado. E por deixar meus dias mais repletos de luz e felicidade.

Ao meu irmão Renner Ribeiro da Silva, meu melhor amigo e maior apoiador.

Aos meus sogros Ronaldo Martins Ferreira e Maria de Fátima Colucci Goulart dos Santos por todo carinho e apoio durante o curso.

Ao meu orientador e admirado professor Sérgio Marcos Carvalho de Ávila Negri, por todas as oportunidades de aprendizado na orientação e nos estágios, sempre me amparando com generosidade e paciência.

Aos colegas de curso do mestrado pelas trocas de conhecimento e debates enriquecedores.

Aos demais professores docentes do programa, sempre dispostos e prestativos em ensinamentos que levarei por toda à vida.

À querida Vanilda Cantarino que por todo apoio e auxilio durante o curso.

A todos os alunos do 7º período do curso de Direito de 2016 da UFJF, pela graciosidade que me receberam durante o estágio.

Muito obrigado.

EPÍGRAFE

A proteção de dados constitui não apenas em um direito fundamental entre outros: é o mais expressivo da condição humana contemporânea.

Stefano Rodotá

RESUMO

A presente dissertação analisará o direito à proteção de dados na sociedade de informação brasileira. O pensamento do jurista italiano Stefano Rodotà sobre as transformações do direito à privacidade, que não é mais compreendido como o direito de ser deixado só, será utilizado. Assim, o direito à privacidade é agora entendido como o direito à autodeterminação informativa, ou seja, o direito que o cidadão possui para controlar dados e informações nas diversas inovações tecnológicas que o permeia. E diante destas transformações, torna-se necessário ter uma correta legislação sobre esse tema.

Palavras-chave: Proteção de dados. Privacidade. Direito fundamental. Internet.

ABSTRACT

The present dissertation will analyze the right to data protection in the Brazilian information society. The thought of the Italian jurist Stefano Rodotà about the transformation of the right to privacy, that is no more comprehended as the right to be let alone, will be used. Thus, the right to privacy is now understood as the right to informative autodetermination, that is, the right that the citizen has to control data and information in the various technologic innovations that permeate him. And in the face of these transformations, becomes necessary to have a correct legislation about this theme.

Keywords: Data protection. Privacy. Fundamental right. Internet.

SUMÁRIO

INTRODUÇÃO

A presente dissertação propõe-se à reflexão acerca do direito à proteção de dados pessoais no Brasil a partir das transformações da privacidade na sociedade de informação.

Desse modo, as mudanças tecnológicas acarretaram uma nova ótica sobre a privacidade, que não pode mais ser compreendida meramente como o direito a ser deixado só, ganhando, assim, uma dimensão de autodeterminação informativa.

A fim de compreender essas modificações na privacidade, bem como o impacto causado pelas tecnologias de computação em rede e internet, esse estudo ampara-se no pensamento do renomado jurista italiano Stefano Rodotà.

Desse modo, a compreensão do autor também atua como alicerce de toda a análise das transformações ocorridas nos direito à privacidade com a ascensão da internet e o surgimento do direito à proteção de dados.

Assim, a dissertação em tela é composta por quatro capítulos: (i) a privacidade: entre velhas ideias e novos problemas; (ii) as novas demandas da privacidade na sociedade de informação; (iii) a teoria da proteção de dados; e, por fim, (iv)a proteção de dados no Brasil.

O primeiro capítulo problematiza a definição tradicional de privacidade como um direito de ser deixado só a partir de digressões históricas sobre a sua origem. Além disso, aborda-se a ideia do direito à privacidade como um direito humano e fundamental propagador da dignidade humana.

Já o segundo capítulo trata do conceito de sociedade de informação e dos impactos desta na noção clássica do direito à privacidade. Aborda-se a sua transformação de um direito contido na esfera individual para uma dimensão intersubjetiva devido à massificação na circulação de informações e dados pessoais proporcionada pela computação em rede. Problematiza-se, ainda, a realidade brasileira na sociedade de informação.

Por seu turno, o terceiro capítulo traz a proteção de dados pessoais como um direito fundamental, bem como um estudo sobre sua teoria, seus princípios e gerações legislativas que dele trataram. Almeja-se demonstrar que o direito à proteção de dados não é uma espécie do gênero privacidade, mas um direito próprio que garante o exercício da nova dimensão da privacidade em uma noção de autodeterminação informativa. Nesse capítulo há também uma abordagem sobre a *General Data ProtectionRegulation* (GDPR), a mais recente regulamentação sobre proteção de dados na União Europeia.

Finalmente, o quarto capítulo busca uma análise dos quadros legislativo e doutrinário da proteção de dados no Brasil, desde sua tutela “indireta” pela ordem constitucional até as

legislações mais atuais, tais como o Código de Defesa do Consumidor (Lei n. 8.078/1990), o Marco Civil da Internet (Lei n. 12.965/2014), o Decreto-Lei n. 8.771/2016 e o Projeto de Lei n. 5.276/2016, que dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural.

A metodologia utilizada foi revisão bibliográfica de obras, artigos e pesquisas referentes ao tema, além das análises constitucionais e legislativas sobre aprivacidade e a proteção de dados no Brasil.

1. A PRIVACIDADE: ENTRE VELHAS IDEIAS E NOVOS PROBLEMAS

Atividades cotidianas que anteriormente se realizavam no convívio social agora envolvem o uso de ferramentas e aplicações pela internet. Tornou-se comum o uso de smartphones e computadores na realização de compras e interações em sites ou aplicativos como *ifood, Facebook, Mercado Livre, Whatsapp, Tinder* entre tantos outros.

Desta forma, uma simples compra de um lanche, uma conversa com amigos e quase todos os afazeres diários apresentam-se ligados ou com a possibilidade de estarem ligados ao uso incessante de tecnologias de rede e comunicação.

A construção da personalidade humana perante o mundo não mais se limita em um campo individual, mas sim a partir de uma intersubjetividade entre indivíduos que, em tempos presentes, perpassa os meios digitais de comunicação. Não por menos, a tutela deste sujeito deve se realizar "em relação com outros (o sentido da alteridade) e com o mundo a ele externo. Hoje se sabe que o ser humano existe apenas como integrante de uma espécie que precisa de outro(s) para existir (*rectius*, coexistir)" (MORAES, 2010, p.14).

Para a realização destas interações pela internet necessariamente os usuários necessitam de "disponibilizar" informações pessoais que os identifiquem e os diferenciem para a própria realização de tais serviços. Isso ocorre pelo compartilhamento de seus "dados pessoais".

Dados pessoais, ou *data,* são informações que podem ser coletadas e tratadas por meios eletrônicos. São utilizadas por empresas ou órgãos públicos para determinado fim comercial, como o uso para uma publicidade, ou para análises de políticas públicas em geral.

Esses dados pessoais são estruturados de forma a significarem para terceiros uma representação virtual do indivíduo – ou *profile* – e são utilizados a fim de aperfeiçoar serviços e ganho de celeridade. Assim, tornam-se possíveis operações cadastrais diversas, trabalhos em *Workstations* e o controle remoto de máquinas à distância em tempo quase real, o que torna mais eficientes, dinâmicas e práticas que anteriormente demandariam muito mais tempo.

Não por acaso, no final de 2016, foi aberta consulta pública acerca da chamada "internet das coisas" [1], que envolve aplicações de objetos que se comunicam e interagem de

[1] Conforme informado no site oficial: Em sua definição mais ampla a Internet das Coisas engloba todos os objetos que transmitem informações através da internet, como computadores, tablets e smartphones. A definição mais estrita, e comumente aceita, considera apenas os objetos capazes de detectar (através de sensores), transmitir informações e atuar sem a presença constante de intervenção humana. No entanto, quando analisamos a Internet das Coisas, devemos nos atentar ao fato de que ela está inserida em um ecossistema, do qual as "coisas" são apenas uma pequena parte dele. Fazem parte deste ecossistema os atores que contribuição para a viabilização da internet das coisas, tais como: empresas, startups, universidades, ICTs, órgãos e esferas

forma autônoma via internet, permitindo o monitoramento e gerenciamento desses dispositivos via *software* para aumentar a eficiência de sistemas e processos.

Essas novas interações intersubjetivas por meios digitais e a expansão global da internet permitem a manipulação de informações pessoais em grande escala. Surgiram empresas e instituições públicas capazes e dispostas a coletá-las, moldá-las e empregá-las na transformação do mundo e na geração de outros conhecimentos e bens a partir da utilização dos dados pessoais eletrônicos.

Por conseguinte, a manipulação da informação pessoal ganhou proeminência na sociedade, pois todo o registro de representação e atividades realizadas pelas pessoas através de seus "avatares" nos meio eletrônicos se tornou altamente valorizado e disputado.

Consagrou-se na sociedade um novo processo de personalização digital, mecânico, informacional, do indivíduo, "desembaraçado dos pesados processos da massificação, reificação e repressão que permitiu a customização da existência, vez que os valores são aceitos a partir do diálogo e não da coerção" (BAIÃO; GONÇALVES, 2015, p. 04). Deste modo, a personalidade se tornou "customizada" em cada interação por essas tecnologias, ou seja, construída a partir de retratos digitais de cada ato realizado na internet, que em conjunto formam uma composição que definem a individualidade de cada usuário.

Contemporaneamente, "o compartilhamento de informações pessoais é da própria natureza da atividade social e também é parte estrutural das redes sociais *online"* (DONEDA, 2012, p. 07). Enquanto nas interações sociais "tradicionais", os meios culturais e tecnológicos já são conhecidos e abalizados, nos meios de comunicação em rede ainda há uma profunda indeterminação sobre a tecnologia que envolve o compartilhamento de dados.

Todavia, com o aumento em escala de tecnologias e ofertas de serviços que se amparam nos dados pessoais, CaitlinMulholland (2012, p. 03) aduz que existe "uma expansão das formas potenciais de violação da esfera privada, na medida em que se mostra a facilidade por meio da qual é possível o acesso não autorizado de terceiros a esses dados".

Intrinsecamente, conforme explicita Rodotá (2008, p. 24), parece ser cada vez mais frágil a definição de "privacidade" exclusivamente como "*The right to be let alone*" (direito de ser deixado só) que decai em prol de novos entendimentos cuja base é representada também pela possibilidade de cada um controlar o uso dos dados pessoais que lhe dizem respeito.

---

governamentais, etc. Disponível em: <http://www.participa.br/cpiot/o-que-e>. Acesso em 13 de fevereiro de 2017.

Assim, sem uma correta regulamentação sobre a privacidade, corre-se o risco de que informações pessoais mais reservadas possam ser reveladas com maior facilidade sem o conhecimento ou a autorização do usuário por esse acesso indevido aos dados pessoais.

1.1. DA INTIMIDADE À PRIVACIDADE: A INÓCUA DISTINÇÃO TERMINOLÓGICA PARA A PROTEÇÃO DE DADOS

Antes mesmo de se adentrar ao estudo das mudanças da privacidade, é imperioso abordar o direito à intimidade pela estreita relação que ambas possuem e, criticamente, analisar se tem sentido prático aderir a uma distinção.

A privacidade e a intimidade possuem guarida constitucional[2], inclusas no rol de garantias e direitos fundamentais, não podendo, pois, ser objeto de discussão por emendas constitucionais no Brasil, uma vez que são cláusulas pétreas[3], conforme o inciso IV do §4º do artigo 60 da Constituição Federal de 1988 (CF/1988).

Nesse sentido, Felipe Kersten e Alessandra Mistrongue (2004, p. 314) explanam que a intimidade é enxergada como o direito que protege o íntimo, os segredos pessoais e a liberdade de praticar determinados atos e ações sem que outros saibam ou julguem. O direito à intimidade objetiva resguardar os indivíduos dos conceitos morais alheios, fundando-se principalmente no direito à liberdade, também fundamental.

A intimidade, como um direito da personalidade do indivíduo, é a garantia de que o mesmo não passe de mero ator social submetido às forças econômicas e sociais. Assegura uma dimensão de liberdade de "ser" no âmbito privativo, secreto ou exclusivo. Isso ocorre com o objetivo de salvaguardar o exercício de direitos individuais não compartilháveis de potenciais ofensas pelo Estado ou entes privados[4].

Já o direito à privacidade é distinto do direito à intimidade, sendo uma esfera mais ampla na qual a intimidade está contida. Relaciona-se ao exercício de liberdades individuais

---

[2]Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

[3]De acordo com o artigo 60, §4º, da Constituição Federal de 1988, "não será objeto de deliberação a proposta de emenda tendente a abolir: I - a forma federativa de Estado; II - o voto direto, secreto, universal e periódico; III - a separação dos Poderes; IV - os direitos e garantias individuais".

[4]Não por menos o artigo 21 de o Código Civil expressa ser a vida privada da pessoa natural inviolável e, desse modo, o juiz, a partir do requerimento do interessado, irá adotar as necessárias providências a fim de impedir ou fazer cessar ato contrário a esta norma.

nas interações intersubjetivas protegidas pelo Estado. Privacidade e intimidade não se confundem, pois a primeira, como gênero da segunda, é constituída por elementos psíquicos que o indivíduo divide nas relações sociais e que também devem ser ocultas a terceiros que delas não participam.

A utilização da tutela da privacidade serve para distinguir a dimensão individual de cada pessoa em suas interações sociais, salvaguardando suas liberdades de terceiros com os quais eventualmente possa se opuser. Distintamente da intimidade, é a tutela da privacidade que resguarda a imagem, honra ou a identidade pessoal em suas dimensões individuais nas relações intersubjetivas, sendo amplo o bastante para guarnecer todo este conteúdo (DONEDA, 2008, p. 05).

Porém, para efeitos práticos, tanto em doutrina como na práxis dos tribunais possuem o mesmo tratamento jurídico. A intimidade, embora "espécie" do "gênero" privacidade não obtém na prestação jurídica razões fáticas que ensejem uma distinção ou proteção detalhada da mesma, sendo pacificamente protegida pela própria tutela da privacidade.

Demonstrando quão inócua é a distinção terminológica em nosso ordenamento, pelo menos em relação à aplicação em tribunais, Daniel Bucar (2016, p. 80), ao elencar estatísticas jurisprudenciais relativas aos julgados pelo STF e STJ em que são invocados os vocábulos privacidade e intimidade, demonstrou ser indefinido e indistinto o uso dos mesmos, que se misturam e vão desde sigilo bancário até divulgação indevida de imagens e dados pessoais em mídias diversas.

Assim, além da inexistência na jurisprudência de distinção clara acerca do que se entende por privacidade ou intimidade, a estatística desses julgados demonstra uma tendência de manejo do conceito de ambas visando uma tutela patrimonial da privacidade do indivíduo.

Destarte, esta indefinição serve para a defesa da privacidade como um direito de propriedade contra a aplicação invasiva de normas relativas a "a) exigência de tributos; b) investigação de crimes contra o patrimônio público; e c) cumprimento de obrigações pecuniárias assumidas entre particulares" (BUCAR, 2016, p. 100).

Para fins do presente estudo, torna-se ineficaz assumir distinções especificas entre a privacidade e a intimidade, pois ambas são guarnecidas pela mesma tutela dos direitos fundamentais no Brasil que se entrelaçam e se confundem. Portanto, deverão ser respeitas e tuteladas simultaneamente por qualquer legislação de proteção de dados.

1.2 DA INTIMIDADE AO DIREITO DE FICAR SÓ: DIGRESSÕES HISTÓRICAS SOBRE A PRIVACIDADE

Antes de problematizar a aplicação e a utilização do direito à privacidade na sociedade contemporânea de informação, é imperioso refletir sobre a sua mudança conceitual, envolvendo desde quando ainda era basicamente o direito ao foro íntimo até o chamado "*The right to be let alone*" ou o direito de ser deixado só.

Especificamente sobre a origem histórica da privacidade, esta inicialmente se mesclava com o direito à intimidade. Segundo Alice Monteiro de Barros (1997, p. 19), a sua própria noção para o direito teria sua origem bastante debatida e envolta em dissenso entre os estudiosos. Diz a autora:

> Alguns autores da chamada corrente histórica acreditam que a intimidade existia nas civilizações antigas, pois seria uma característica inata ao homem que àquela época já distinguia o mundo político do privado. Assim, essa distinção era nítida uma vez que todo e qualquer assunto que relacionasse o individuo ao público seria parte do mundo da política, enquanto que tudo aquilo que era individual e secreto pertencia ao mundo privado, esfera aonde se exercia a intimidade (BARROS, 1997, p. 19).

Porém, segundo Bucar (2016, p.110), o início da tutela da intimidade como conhecemos surgiu apenas com o fim do Feudalismo e a ascensão da burguesia em sua luta contra o Estado Absoluto. Desse modo, a conceituação jurídica da mesma estaria atrelada ao ideário de propriedade privada e ao modo de vida burguesa contra o desejo de controle pelo Estado.

Corroborando esse entendimento, Edoardo Giannotti (1987, p. 14) defende ser praticamente impossível localizar a noção de tutela da intimidade, ou sua reivindicação em civilizações anteriores, como gregas ou romanas, uma vez que não existiriam as mesmas pressões sociais que estimulassem o indivíduo ao isolamento e ao próprio lar ou casa. Aliás, o lar de um *pater familias* e de sua família era habitada por indivíduos diversos em castas e classes, não se confundindo com o ideário da família burguesa.

Em consonância, Rodotá (2008, p.26) menciona em sua obra uma observação de Lewis Munford, segundo o qual a primeira mudança radical no lar medieval rumo à Modernidade foi o aparecimento do sentimento de intimidade, isto é, de cada indivíduo por vontade própria se afastar da coletividade para refeições, sono, intimidade sexual ou prática religiosa.

Essa necessidade de afastamento temporário e de isolamento para determinadas atividades, marcaria profundamente a casa feudal, uma vez que eventos ou ações antes

realizadas por diversos estratos sociais em comunidade acabariam por se tornar atos cada vez mais individualistas, em perfeita sintonia com o ideário de vida burguês. Basta pensar que o isolamento geralmente era associado com o descanso, sendo privilégio de pouquíssimos escolhidos que dispunham de bens materiais para garantir essa intimidade.

O exercício da intimidade burguesa projetou anseios de resguardo a outras dimensões e direitos pessoais nas relações sociais, construindo uma necessidade de tutela daquilo que hoje compreendemos como privacidade. Segundo Rodotá (2008, p.27) "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". Não por menos, a construção jurídica da privacidade espelhou-se no desejo burguês de se isolar cada vez mais da classe operária e da comunidade.Conforme Rodotá (2008, p.27):

> A realização das condições materiais para a satisfação da necessidade de intimidade surge como um momento mais complexo, através do qual a burguesia reconhece a própria identidade no interior do corpo social. A possibilidade de aproveitar plenamente a própria intimidade é uma característica que diferencia a burguesia das demais classes: e o forte componente individualista faz com que esta operação se traduza posteriormente em um instrumento de isolamento do indivíduo burguês em relação à sua própria classe. O burguês, em outros termos, apropria-se de um seu "espaço", com uma técnica que lembra aquela estrutura para a identificação de um direito à propriedade solitária.

Dessa forma, a dinâmica da privacidade se tornou imanente às reflexões desta classe que destacou o seu modo de viver como o centro normativo das legislações. Forçou-se a atenção para aspectos do cotidiano burguês, como se evidenciou no texto do artigo 2º da Declaração dos Direitos dos Homens e do Cidadão de 1789: "o fim de toda associação política é a conservação dos direitos naturais e imprescritíveis do homem. Esses direitos são a liberdade, a propriedade, a segurança e a resistência à opressão" (BUCAR, 2016, p.151).

A fim de se viver em sociedade, era necessário garantir a qualquer indivíduo o exercício de seus direitos patrimoniais e de liberdades, desvencilhando-os do arbítrio e controle das forças políticas e estatais em pelo menos parte de seu dia a dia. Para tanto, no século XIX, a propriedade se tornou essencial para o desenvolvimento da pessoa em sua personalidade, uma vez que para se acessar aos direitos era necessário se equiparar ao burguês.

A necessidade de ser ter propriedade para exercer a privacidade favoreceu a burguesia e outras classes dominantes em detrimento dos menos abastados. A privacidade era atribuída à proteção da propriedade privada, da imagem privada ou da honra do lar.

Tal quadro se perpetuou e foi fortalecido pela revolução industrial na transição para a Modernidade, com a ascensão da burguesia industrial à classe mais influente nos rumos da comunidade e a consagração do Liberalismo na política e economia, em meados do século XIX.

Mas embora a privacidade tenha raízes burguesas e sua forma esculpida para atender precipuamente àquela classe, é certo que gradualmente foi se capilarizando por todo o tecido social, estendendo-se inclusive para a classe operária[5]. Neste sentido de prerrogativa da classe burguesa, "o direito à privacidade passou a ter como titular qualquer pessoa do povo, proprietária ou não, deixando de revestir o muro de separação fincado entre a burguesia e a massa" (BUCAR, 2016, p. 246).

Isso graças a motivos diversos, tais como demandas trabalhistas e sociais até uma maior amplitude e crescimento do fluxo de informações com o fortalecimento da imprensa. A expansão do direito à privacidade para todas as classes vai se desvencilhando da noção de um direito patrimonial para um direito atrelado à personalidade humana.

O marco formal desta virada hermenêutica remonta ao artigo "*The right to privacy*" de Samuel Warren e Louis Brandeis. Em breve síntese,no artigo em questão, os autores definiam a privacidade como o "direito de ser deixado só" atrelado à personalidade, distinguindo o mesmo do direito de propriedade de bem íntimos[6]. Esclarece Doneda (2006, p.136) que o texto "reflete a tendência a uma fundamentação diversa para a proteção da propriedade, que começa a despontar".

No final do século XIX, com o desenvolvimento da imprensa e o seu interesse sobre hábitos e detalhes íntimos de personalidades de expressão da época, os autores perceberam que não deveriam mais as invasões sobre a intimidade da pessoa serem tratadas como mero dano de propriedade ou questões legais de direitos autorais. Mas sim como ações que geram dano no indivíduo em sua personalidade, além da esfera material comum.

---

[5]"Ao individualismo soma-se, portanto, os meios materiais que, em um primeiro momento, estavam à disposição da burguesia e que foram posteriormente massificados; meios estes que providenciaram de várias formas a delimitação de espaços entre ocupantes de uma mesma casa" (DONEDA, 2008, p.133).

[6]*These considerations lead to the conclusion that the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone. It is like the right not be assaulted or beaten, the right not be imprisoned, the right not to be maliciously prosecuted, the right not to be defamed. In each of these rights, as indeed in all other rights recognized by the law, there inheres the quality of being owned or possessed -- and (as that is the distinguishing attribute of property) there may some propriety in speaking of those rights as property.But, obviously, they bear little resemblance to what is ordinarily comprehended under that term. The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality*(WARREN; BRANDEIS, 1989, p.193).

Um dos pontos fundamentais apontados por Warren e Brandeis é que o princípio a ser observado na proteção da privacidade não passa pela propriedade privada, mas pela chamada "*inviolatepersonality".* Trata-se de um direito de natureza pessoal que possui o "eixo entorno da proteção da pessoa humana que será determinante na proteção da privacidade no século seguinte" (DONEDA, 2006, p.136).

De certo modo, o "*right of privacy"* defendido por Warren e Brandeis buscava defender pequenos núcleos comunitários, como famílias ou associações religiosas, separando suas atividades íntimas da sociedade industrial que despontava "com o intento de preservar uma referência para a identidade da classe e o individualismo pessoal" (BUCAR, 2016, p.216).

Assim, o direito à privacidade se apresentava ligado à pessoa humana, porém, ainda como um direito individualista, que distinguia o tutelado da comunidade a que estava inserido. Esse "império" da privacidade como um direito de ser deixado só exigia do Estado Nacional a proteção irrestrita em prestações negativas, dimensão que até hoje é presente nas legislações vigentes.

A expansão da noção de que caberia ao Estado impedir a ofensa à intimidade e à privacidade, com a transição do Estado Liberal para o *welfarestate* ou Estado de Bem Estar Social, assumiu a projeção normativa de privacidade como um direito fundamental atrelado à dignidade humana.

Desde esse marco inicial até os dias presentes, a privacidade ainda é reconhecida como um direito de preservar um espaço ou esfera íntima de cada pessoa para seu desenvolvimento pleno da personalidade, que não deveria ser compartilhada com o mundo e merecedora de proteção do Estado.

1.3 O DIREITO À PRIVACIDADE: DIREITO HUMANO E FUNDAMENTAL PROPAGADOR DA DIGNIDADE DA PESSOA HUMANA

Antes da Segunda Guerra Mundial, as constituições centravam-se nas questões relativas à vida pública enquanto as relações privadas eram regidas pelos grandes códigos civis que se ocupavam das propriedades, da família e dos direitos privados do indivíduo. Isso se alterou profundamente com o pós-guerra.

Diversos aspectos das relações privadas, anteriormente regidas por códigos e legislações civis infraconstitucionais, foram "constitucionalizados", fazendo parte dos textos constitucionais inclusive no Brasil (NEGRI; MACHADO, 2016, p.122).

Após a Segunda Guerra Mundial, a privacidade manteve o cunho individualista, mas diferente da ideia patrimonialista de antes, se ocupou da dimensão humana, recebendo abrigo em diversos tratados e legislações internacionais.

Segundo Doneda (2006, p. 09), a primeira menção do direito à privacidade como direito humano foi em 1984, na Declaração Americana dos Direitos e Deveres do Homem. No mesmo ano, também se apresentou na Declaração Universal dos Direitos do Homem, aprovada pela Assembléia Geral das Nações Unidas em 1948, além da Convenção Europeia dos Direitos do Homem, em 1950. Ainda, na Convenção Americana dos Direitos do Homem, conhecida como "Carta de San José", de 1969 e, mais recentemente, na Carta dos Direitos Fundamentais da União Europeia (2000).

Por conseqüência das atrocidades vivenciadas e pelos horrores causados pela Segunda Guerra Mundial, as nações que pregavam valores democráticos no ocidente perceberam a importância de se afirmarem direitos humanos universais para a concretização do que entendiam por justiça. Dentre esses estava a privacidade.

O Direito – que se alicerçava na formalidade e rigor de um direito positivo e patrimonial – por muitas vezes acabava sacrificando a justiça em prol de uma segurança jurídica. Em resposta aos problemas enfrentados por essa concepção positivista do Direito na guerra, com a instrumentalização e relativização do ser humano, o mundo jurídico traz para o epicentro da ciência uma maior atenção às necessidades de proteção dos direitos fundamentais e da própria dignidade humana.

Os ordenamentos passam a valorizar em seu epicentro a tutela da pessoa natural. Desse modo, não é possível "coisificar" o ser humano. Pela condição humana, a pessoa natural passa a ser enxergada como dotadade dignidade, uma qualidade intrínseca e indissociável de todo e qualquer indivíduo e, portanto, todo o arcabouço jurídico nele passou a se pautar e convergir.

Aliás, essa pretensão de dignidade centrada no próprio homem surge por influência kantiana. Kant (2007, p.68) aduz que:

> O homem, e, duma maneira geral, todo o ser racional, existe como fim em si mesmo, não só como meio para o uso arbitrário desta ou daquela vontade. Pelo contrário, em todas as suas ações, tanto nas que se dirigem a ele mesmo como nas que se dirigem a outros seres racionais, ele tem sempre de ser considerado simultaneamente como fim.

Considera-se o ser humano como a unidade nuclear, pois reconhece igual capacidade em todo indivíduo, "capaz de produzir um conceito geral sobre as coisas, representando

mentalmente o objeto, abstraindo-lhe ou transcendendo-lhe as particularidades" (MACHADO; NEGRI, 2011, p.191).

Fundamentalmente, para Kant os seres humanos possuem um valor que os torna acima de tudo, detentores de dignidade. Esta é a razão do mesmo afirmar que o homem, como ser não pode ser usado como meio para se alcançar um fim, ainda que visando ao bem-estar da maioria[7]. De tal modo, o Direito passa a ser enxergado como instrumento feito pelo homem para o homem e como tal, assegura o status jurídico compatível à sua existência humana.

A partir do pós-guerra, com o advento das Declarações de Direitos do Homem, se esculpiram as normas constitucionais contemporâneas, com os valores morais sobre a dignidade humana com status de universalidade e obrigatoriedade e garantidora de direitos da personalidade[8].

A partir deste momento o direito a privacidade - assim como outros direitos da personalidade – passou a ser um direito humano por ser imanente à natureza humana em si, essencial ao desenvolvimento pleno da pessoa e de sua vivência em sociedade.

Consoante essa compreensão, o nosso ordenamento pátrio elencou o princípio da dignidade humana no artigo 1º, inciso III, da CF/1988[9], como um dos fundamentos da República Federativa do Brasil, que estabelece todos como merecedores de igual proteção de sua dignidade pelo simples fato de serem pessoas humanas. A dignidade da pessoa humana encontra-se no epicentro da ordem jurídica brasileira sendo razão fundamental para a estrutura de organização do Estado e para o Direito constituído como categoria de princípio fundamental da República.

A dignidade da pessoa humana no ordenamento brasileiro é um atributo próprio à pessoa justamente devido à mesma ser dotada de humanidade, tendo caráter de

---

[7]Trata-se, de formulação importante do imperativo categórico kantiano, princípio moral fundamental do qual todas as nossas obrigações e responsabilidades devem derivar. É impossível conceber a pessoa humana de uma forma inteiramente desprovida de valores, instrumentalizando-a (STANCIOLI, 2010, p. 92).

[8]"Aliás, não é outro o entendimento que subjaz ao artigo 1º da Declaração Universal da ONU (1948), segundo o qual "todos os seres humanos nascem livres e iguais em dignidade e direitos. "Dotados de razão e consciência, devem agir uns para com os outros em espírito e fraternidade", preceito que, de certa forma, revitalizou e universalizou – após a profunda barbárie na qual mergulhou a humanidade na primeira metade deste século - as premissas basilares da doutrina kantiana" (SARLET, 2007, p. 367).

[9]Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos:
I - a soberania;
II - a cidadania;
III - a dignidade da pessoa humana;
IV - os valores sociais do trabalho e da livre iniciativa;
V - o pluralismo político.
Parágrafo único. Todo o poder emana do povo, que o exerce por meio de representantes eleitos ou diretamente, nos termos desta Constituição.

universalidade[10]. O próprio artigo 5º da CF/1988 assegura os direitos fundamentais – dentre eles a privacidade - tanto aos brasileiros quanto aos estrangeiros residentes no país.

Porém, conforme elucida Judith Martins-Costa (2003, p.113), o conceito de dignidade não é sinônimo de autonomia ou de pessoa, uma vez que não é o Estado garantir e resguardar a vida que atesta à pessoa o exercício de sua autonomia e nem tão pouco sua dignidade. Não há vida digna em uma existência sobre constrições que não sejam razoáveis. E essas constrições podem adotar contornos diversos, desde debilidades físicas, econômicas ou sociais até a restrição da intimidade para o exercício da personalidade.

De tal sorte garantir uma existência digna também passar pelo dever do Estado assegurar a cada indivíduo o livre exercício de sua autonomia e o reconhecimento institucional como igual independente de suas escolhas de vida. Sobre o ponto,

> A proteção da dignidade da pessoa humana não é sinônima de retirada das instituições do espaço no qual o individuo se autodetermina; ao contrário, implica sua presença a fim de proporcionar aos indivíduos não apenas a liberdade de realizar escolhas existenciais fundamentais para o desenvolvimento da sua personalidade, mas também assegurar-lhes a maior autonomia possível, resguardando a liberdade de poder considerar e rever criticamente as razões dessas escolhas entre diferentes formas possíveis de desenvolvimento da pessoa, sem ter necessariamente de permanecer dentro uma identidade particular cristalizada. Para que o indivíduo possa, efetivamente, ser sujeito do seu destino e das suas escolhas, o Estado precisa assegurar que sua autodeterminação seja exercida de forma desimpedida. Ao assegurar a liberdade de escolha, o Estado também precisa assegurar que o seu conteúdo seja preenchido pelo indivíduo (BAIÃO; GONÇALVES, 2015, p. 08).

Assim, a dignidade da pessoa humana, como valor fundamental do ordenamento, não mitigou a esfera de autodeterminação do indivíduo, não se prestando tal norma como um fundamento de controle do Estado em padrões morais da privacidade[11].

Não por menos, a fim de garantir o exercício pleno da autonomia e personalidade de cada indivíduo, a Declaração Universal dos Direitos Humanos, em seu artigo XII [12], expressamente aduz que“ninguém estará sujeito à interferência em sua vida privada”.

Neste contexto, por influência direta da Declaração Universal de Direitos Humanos da ONU, a privacidade foi reconhecida como direito fundamental no Brasil, com sua

---

[10] Tendo em vista que o ser humano constrói a sua personalidade dentro de contextos coletivos, como família, associações, sociedades; a sua proteção, pelo Direito, não pode ocorrer sem que sejam analisados os impactos da vivência em coletividade para o indivíduo e para a sua possibilidade de autodeterminação. (NEGRI, 2016, p. 07)

[11]Não pode levar a se pensar que há uma autorização, mesmo tácita, para a imposição de padrões morais, sob pena de se negar a principal conquista de todo aquele processo: o reconhecimento do direito ao livre desenvolvimento da personalidade (NEGRI, 2016, p. 08)

[12] Art. 12° Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei.

jusfundamentalidade atestada através da proteção inserida na Constituição Federal de 1988, seguindo a tendência internacional.

Desse modo, a privacidade tornou-se, no Brasil, um direito humano, fundamental, e de personalidade[13]. Sendo assim, a inserção dentro de extenso rol, da intimidade, da vida privada, da honra e da imagem das pessoas conforme inscrito em seu artigo 5º, incisos X e XII da CF/1988[14] buscaram promover a sua relação com a dignidade humana, que é elemento basilar de nosso ordenamento jurídico. Dessa ligação decorrem deveres concretos dos órgãos estatais de tutela e a garantia, inclusive, por meio de medidas positivas (prestações), do seu respeito e da sua promoção.

Importante ressaltar, ainda, que essas normas definidoras de direitos e de garantias fundamentais em nosso ordenamento têm aplicação imediata (§ 1º, artigo 5º, CF/1988), não sendo cabível o desrespeito às mesmas ainda que na ausência de leis infraconstitucionais uma vez que são cláusulas pétreas. Ainda, os direitos humanos, por força do § 3º do artigo 5º da CF/1988, são também considerados como cláusulas pétreas no Brasil.

Ecoando a norma constitucional, a legislação infraconstitucional também reconheceu e reproduziu a privacidade como direito da personalidade[15]de cada cidadão, atraindo para ela toda a tutela dessa categoria de direitos. Desta forma, no artigo 11 do Código Civil de 2002(CC/2002) estatui-se que os direitos da personalidade são intransmissíveis e irrenunciáveis.

---

[13] "Muitos dos direitos fundamentais são direitos de personalidade, mas nem todos os direitos fundamentais são direitos de personalidade. Os direitos de personalidade abarcam certamente os direitos de estado (por ex.: direito de cidadania), os direito sobre a própria pessoa (direito à vida, à integridade moral e física, direito à privacidade),os direitos distintivos da personalidade (direito à identidade pessoal, direito à informática) e muitos dos direitos de liberdade (liberdade de expressão). Tradicionalmente, afastavam-se dos direitos de personalidade os direitos fundamentais políticos e os direitos a prestações por não serem atinentes ao ser como pessoa. Contudo, hoje em dia, dada a interdependência entre o estatuto positivo e o estatuto negativo do cidadão, e em face da concepção de um direito geral de personalidade como "direito à pessoa ser e à pessoa devir", cada vez mais os direitos fundamentais tendem a ser direitos de personalidade e vice versa" (CANOTILHO, 2003, p. 396).

[14] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

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

XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

[15] "A proteção da privacidade, elemento indissociável da personalidade, merece esta tutela integrada, sendo provavelmente um dos casos em que ela é mais necessária. A cotidiana redefinição de forças e meios que possibilitama intromissão na esfera privada dos indivíduos demanda uma tutela de caráter incessantemente mutável. Sintetizando, a privacidade, incluindo em seu bojo a intimidade, é direito da personalidade inviolável, irrenunciável, imprescritível e intransmissível por força do Código Civil de 2002 e, também, um direito fundamental humano por estar previsto no artigo 5º da Constituição" (DONEDA, 2000, p.128).

A esses atributos a doutrina ainda acrescenta os de caráter absoluto, de generalidade e de imprescritibilidade (BUCAR, 2016, p.347). Consta ainda no artigo 20 do Código Civil que - salvo exceções expressas em lei – os direitos de imagem, publicação de escritos e divulgação de palavras uma pessoa "poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se destinarem a fins comerciais".

Em complemento, o artigo 21 do CC/2002, expressamente afirma que: "a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma".

Conforme destaca Bucar (2016, p.415), em relação ao conteúdo da privacidade, tanto a doutrina brasileira como estrangeira se concentram em concepções variadas e diversas, mas não mais atreladas a uma ideia patrimonialista[16].

O autor (BUCAR, 2016, p.415) as organizou em: direito de ser deixado só; direito de limitação de acesso a questões pessoais; direito ao segredo; direito de efetuar as próprias escolhas existenciais sem controle público ou estigmatização social; direito de manter o controle das próprias informações e de determinar livremente como construir a própria esfera privada; direito de não ser simplificado, transformado em objeto, valorado fora de um contexto.

Contemporaneamente, por parte da doutrina e jurisprudência, a defesa da privacidade no Brasil já se ampara sobre essas novas concepções. Não por menos os controles espacial, contextual e temporal dos dados e informações pessoais forma reconhecidos, conforme determinação do enunciado 404[17] aprovado na V Jornada de Direito Civil do Conselho da Justiça Federal. Sobre o mesmo,

> Assim, como se vê, a privacidade não mais pode ser identificada como questão de sigilo, dentro do qual o indivíduo se isola para viver à margem de todo o tecido social. Não mais sendo possível a coexistência nesse sentido, a imbricação do ser humano na sociedade se dá, inevitavelmente, por meio da circulação de suas informações pela rede de relacionamentos pessoais e institucionais, o que clama pela alteração de perspectiva da privacidade para o controle espacial e contextual das

[16] "(...) dentre as garantias oferecidas ao sujeito, reconhece-se a prevalência, sobre o patrimônio, da proteção da personalidade humana, seja no que diz respeito à sua identidade e à sua integridade, seja no que se refere à sua intimidade e à sua vida privada. Tais bens, de fato, passaram a constituir os pontos cardeais de nosso sistema jurídico, o qual, porém, tem sido sistematicamente bombardeado e desafiado – assim como vem ocorrendo em todos os cantos do mundo – por inovações científicas e tecnológicas de grande magnitude e de consequências aparentemente imprevisíveis, incontroláveis e inevitáveis" (MORAES, 2010. p. 122).

[17] Enunciado 404: A tutela da privacidade da pessoa humana compreende os controles espacial, contextual e temporal dos próprios dados, sendo necessário seu expresso consentimento para tratamento de informações que versem especialmente o estado de saúde, a condição sexual, a origem racial ou étnica, as convicções religiosas, filosóficas e políticas.

> próprias informações, convergindo, portanto, em ampla disciplina de proteção de dados pessoais. (BUCAR, 2016, p.655)

Apesar disso, esses controles ainda se encontram raros nos textos legislativos brasileiros. Talvez porque "a tendência de se legislar sobre dados pessoais, no entanto, não gerou ressonância perceptível no ordenamento jurídico brasileiro até pouco tempo" (DONEDA, 2015, p. 370), o que justifica um aprofundamento na temática em busca de formulações pertinentes à realidade local[18].

Ocorre que essas construções doutrinárias e jurisprudenciais não são errôneas, mas insuficientes. É necessário que essa mudança de perspectiva alcance a legislação, que funcione como um marco civilizatório. Que reconheça formalmente que na sociedade de informação, a busca pela tutela e promoção do direito à privacidade não pode mais ser enxergada apenas em um prisma individualista e subjetivo, uma vez que a própria personalidade humana se projeta por meio da tecnologia.

[18] "Hoje se pode afirmar que já não nos encontramos em um cenário no qual a regulação da proteção de dados pessoais somente interesse a países que apresentavam papel de relevante desenvolvimento econômico e tecnológico. A penetração dos processos de tratamento automatizado de informações pessoais tornou-se regra, tanto é que ao final de 2014, podem ser contabilizados 101 países que possuem suas próprias leis de proteção de dados pessoais" (DONEDA, 2015, p.370).

2. AS NOVAS DEMANDAS DA PRIVACIDADE NA SOCIEDADE DE INFORMAÇÃO

Diversas – e até certo ponto confusas – são origens da conceituação de sociedade de informação contemporânea. Para fins do presente estudo, aborda-se o raciocínio de Armand Mattelart[19],que sobre tamanha obscuridade, afirma:

> Não é meu objetivo aqui retroceder à história de longa duração de uma sociedade guiada pela "informação", surgida bem antes do aparecimento do conceito. Eu me limitarei a destacar aquilo que o pensamento contemporâneo deve ao período que abre a segunda guerra mundial. Primeira fase: os anos cinquenta/sessenta. Tendo como pano de fundo o confrontobipolar Leste/Oeste se delineiam, no seio do *establishment* sociológico americano, as premissas teóricas sobre a "sociedade pós-industrial", alternadamente designada como "sociedade pós-histórica", "pós-capitalista", "tecnotrônica", etc. Instaura-se, ainda, um discurso de acompanhamento sobre a sociedade futura, orientada pelo primado da ciência e da técnica, fundamentalmente informacional: o discurso dos "fins".

Assim, a questão sobre o início desse período presente é o menos relevante, pois são flagrantes suas características. Se fosse necessário simplificar a conceituação do que seria uma "sociedade de informação", basicamente seria uma sociedade aonde há o primado da criação e circulação de informação.

Nela a própria pessoa humana se representa por dados digitais e signos em atividades – cotidianas ou mercantis – por meios eletrônicos de comunicação. Daí porque a conformação social que opera nesse lastro venha a ser chamada de sociedade da informação, uma vez que:

> A fonte da produtividade nas sociedades contemporâneas, portanto, é a aplicação de técnicas e tecnologias no processamento de informações para a geração de novos conhecimentos, assim como a aplicação destes conhecimentos no processamento de outras informações, formando um círculo virtuoso (GHISI; PEZZELA, 2015, p. 04).

Na sociedade de informação, a pessoa primeiramente se apresenta por uma representação sua "conhecida por dados, números, rotinas de compras e gastos, na forma de textos, imagens, sons e dados registrados" (PEZZELLA (2013, p. 234). De tal modo, a existência humana é expressa e sintetizada em dados, que são processados por meios eletrônicos, monitorados global e diuturnamente por governos e organismos internacionais e, ainda, vendidos como recurso base.

[19] Palestra de Armand Mattelart na abertura do V Encontro Latino de Economia Política da Informação, Comunicação e Cultura, realizada em Salvador, Bahia, Brasil, de 9 a 11 de novembro de 2005, cujo texto traduzido na íntegra:<http://www.gepicc.ufba.br/enlepicc/ArmandMattelartPortugues.pdf>. Acesso em 13 de fevereiro de 2017.

Esse papel da informação – e, por consequência, dos dados – na sociedade contemporânea não é fruto de um acaso, mas resultado de profundo e gradativo amadurecimento tecnológico. Ao se incrementar a capacidade de armazenamento e comunicação das informações com a computação, estas podem ser processadas e organizadas, ganhando valor mercantil.

Conforme ilustram Baião e Gonçalves, (2014, p. 02):

> A infraestrutura informativa é parte indispensável da organização da sociedade. Contudo, ao lado do acesso aos dados pelas mais variadas tecnologias, sem mitigar a liberdade, torna-se necessário permitir o controle por parte do cidadão.

Consequentemente, na sociedade de informação a privacidade é cada vez mais atrelada ao controle de nossas informações pessoais, ou dados, em ambientes diversos mediante a mudança tecnológica.

A participação e a inclusão nesse novo modelo de sociedade exigem dos indivíduos maior abertura de informações a seu respeito, como, por exemplo, na contratação de um determinado serviço que somente se concretiza a partir do fornecimento de dados pessoais ou, ainda, nas aplicações de um aparelho celular que só funciona a partir do perfil construído pela coleta de seus dados.

É certo que atualmente as novas tecnologias como navegação em nuvem, internet das coisas, convergência, sincronicidade, multiplataformas e aparelhos auxiliam o avanço e a prática do uso da tecnologia e informação. Graças ao progresso tecnológico é possível acessar esses dados, seja por e-mail ou por rede social, em qualquer celular ou computador.

Neste sentido, uma aplicação pertinente e concreta do Direito só será efetiva se considerar a realidade social a qual se está inserido, reconhecendo que essa "realidade" é fatalmente condicionada pelo desenvolvimento tecnológico vivenciado.

Problematizando a relação entre o Direito e a tecnologia, Doneda (2006, p. 55) afirma que "o verdadeiro problema não é saber sobre o que o direito deve atuar, mas sim de como interpretar a tecnologia e suas possibilidades em relação aos valores no ordenamento jurídico". Quando se trata de uma legislação sobre proteção de dados na sociedade de informação, a aplicação do Direito deve ser horizontalizada, pela própria natureza da rede.

Essa nova percepção da realidade do indivíduo como um ser informacional passa a reclamar uma nova análise do ordenamento jurídico sobre a proteção ao direito à privacidade. Notadamente por "se tratar de um direito fundamental de primeira grandeza reconhecido

como direito de personalidade, com caracteres de indisponibilidade, intransmissibilidade, inalienabilidade e imprescritibilidade" (PEZZELLA, 2013, p. 234).

A convivência humana na sociedade de informação se dá por meio da entrega e distribuição de informações pessoais pela internet. Isso"clama pela alteração de perspectiva da privacidade para o controle espacial e contextual das próprias informações, convergindo, portanto, em ampla disciplina de proteção de dados pessoais" (BUCAR, 2016, p.655-657).

Não por menos, a própria "*General Data Protection Regulation*" (GDPR), que regula a proteção de dados na União Europeia, determina a necessária regulamentação dos dados em uma sociedade de informação para a facilitação do mercado interno[20].

É clara a necessidade de se criar mecanismos jurídicos sobre a proteção de dados, levando conceitualmente em conta a necessária mudança no entendimento de privacidade para um instituto mais relacional que considere a manipulação e coleta de tais dados.

2.1 A PRIVACIDADE NA SOCIEDADE DE INFORMAÇÃO

A consolidação do Estado Social no pós-guerra e o advento da sociedade de informação foram decisivos para a modificação da privacidade, que passou a funcionar contemporaneamente como um instrumento contra a discriminação e favorável às liberdades e igualdades em detrimento de uma visão meramente patrimonial.

Se tradicionalmente a privacidade era o direito de ser deixado só, nos dias atuais ela "evoluiu para incluir em seu conteúdo situações de tutela de dados sensíveis, de seu controle pelo titular e, especialmente, de respeito à liberdade das escolhas pessoais de caráter existencial" (MULHOLLAND, 2012, p. 02). A tutela da privacidade na sociedade de informação reflete necessariamente os efeitos causados pela mesma, quais sejam:

> - passamos de um mundo no qual as informações pessoais estavam substancialmente sob exclusive controle dos interessados para um mundo de informações divididas com uma pluralidade de sujeitos;
> - passamos de um mundo no qual a cessão das informações era, em grande parte dos casos, efeito das relações interpessoais, tanto que a forma corrente de violação da privacidade era a "fofoca", para um mundo no qual a coleta das informações ocorre através de transações abstratas;
> -passamos de um mundo no qual o único problema era o controle do fluxo de informações que saíam de dentro da esfera privada ao exterior, para um mundo no qual se torna cada vez mais importante o controle das informações que entram como

[20] *(17) This Regulation should be without prejudice to the application of Directive 2000/31/EC of the European Parliament and of the Council, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive. That Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States.*

> demonstra a crescente importância assumida pelo direito de não saber, pela atribuição aos indivíduos do poder de recusar interferências em sua esfera privada, como as derivadas da remessa de material publicitário e do marketing direito;
> Vivemos em um mundo no qual aumenta o valor agregado das informações pessoais, com uma mudança de paradigma, onde a referencia ao valor em si e de sua dignidade passou a secundário em relação à transformação da informação em mercadoria;
> - vivemos em um mundo no qual se começa a refletir conscientemente sobre o fato de que, até agora, as tecnologias da informação e da comunicação assumiram muito frequentemente as características de tecnologias sujas, aproximando-se muito mais do modelo das tecnologias industriais poluentes, tornando-se fundamental, portanto favorecer ou impor a introdução no ambiente informativo de tecnologias limpas;
> - vivemos em um mundo no qual as tecnológicas da informação e da comunicação contribuíram para tornar cada vez mais sutil a fronteira entre esfera pública e a esfera privada; e a possibilidade de construção livre da esfera privada e de desenvolvimento autônomo da personalidade passou a ser condições para determinar a efetividade e a amplitude da liberdade na esfera pública. (RODOTÁ, 2008, p.127)

Certamente, uma concepção de propriedade privada suficiente para assegurar a intimidade não subsiste mais na sociedade de informação. As inovações tecnológicas, como câmeras, gravadores, aparelhos de intercepção telefônica e computadores, contribuem decisivamente para que "não só os poderes públicos, mas também particulares, rompam a barreira física da propriedade e possam invadir aspectos mais íntimos da vida pessoal privada" (GHISI; PEZZELA, 2015, p. 04).

Isto posto, com o advento das *big datas* e o avanço tecnológico no manejo de dados, a circulação de informações pessoais passou a ser também utilizada para o desenvolvimento das prestações públicas e serviços privados. E essa circulação mostrou-se generalizada, não mais se ocupando em depurar sobre quem era o proprietário das informações, "o quanto era notória ou não, proprietária ou não, determinada pessoa; as informações sobre ela eram necessárias para o acesso a serviços públicos" (BUCAR, 2016, p. 258). Essa coleta ampla e massiva se tornou cada vez mais habitual em prestações de serviços nas áreas da saúde, da seguridade social ou em qualquer outro campo de atuação do *welfarestate*.

A combinação de diversas tecnologias de automação permitiu a acumulação e o manejo organizado de uma grande quantidade de informação sobre as pessoas e a elaboração de cadastros e perfis virtuais que passaram a fundamentar políticas sociais pelos órgãos públicos ou decisões econômicas por agentes econômicos (MENDES, 2011, p. 45).

E a exigência sobre a disponibilidade dessas informações conduziu a privacidade para além de uma noção de direito negativo, de isolamento, ou de sigilo absoluto da vida privada. A tutela da privacidade passa a ser vista não só como o direito de não ser molestado, mas também como o direito de ter controle sobre os dados pessoais e, com isso, impedir a sua circulação indesejada (MULHOLLAND, 2012, p. 03).

Certamente, com o quadro global apresentado, os quadros institucionais e jurídicos não podem mais considerar os problemas pertinentes à privacidade somente pelo pêndulo constante de "proteger" ou "divulgar" informações de foro íntimo ou de interesse público, uma vez que a privacidade não pode ser mais enxergada como uma dimensão individualista[21].

A privacidade não perde sua natureza ou lógica de exclusão contra ameaças ou controle externo da esfera privada do indivíduo. Porém, na sociedade de informação, ela não tem apenas esta dimensão, mas impõe-se como direito fundamental.

Tornou-se cada vez mais clara a necessidade de eliminar ou mesmo reduzir a ingerência de sujeitos externos na esfera privada das pessoas, de suas informações pessoais, através de textos normativos. Consoante Baião e Gonçalves (2015, p. 04), a sociedade passa a ser "caracterizada, essencialmente, por reduzir as atitudes autoritárias e dirigistas e, ao mesmo tempo, por aumentar a oportunidade das escolhas particulares, a privilegiar a diversidade".

De acordo com Rodotá (2008, p. 25), pela ininterrupta exposição ao mundo digital, pela internet,os cidadãos passaram a ser julgados e representados por dados pessoais em atividades que funcionam e se estruturam como suas identidades virtuais, o que em si não é necessariamente problemático.

Porém, deixa patente que a privacidade não deve ser pensada somente em moldes subjetivos e individuais. Ela deve ser vista como indutora de direitos e liberdades em um contexto tecnológico e informacional expansivo, muito além do sentido de exclusão. Alterou-se profundamente, dessa forma, a função sociopolítica da privacidade para além da esfera individual se tornando elemento constitutivo da cidadania (RODOTÁ, 2008, p. 129).

Conforme foi pontuado, informação na sociedade pós-industrial é recurso base, o que modifica os parâmetros na defesa da privacidade, uma vez que se multiplicaram as possibilidades de manipulação de informações pessoais pelo próprio salto tecnológico da computação.

Neste sentido, conforme ilustra Bucar (2016, p. 261):

> Portanto, na segunda metade do século XX, a informação sobre determinada pessoa já não mais tinha apenas a função de alimentar a curiosidade, por exemplo, de leitores de certa revista acerca dos fatos mundanos de celebridades políticas, artísticas, intelectuais ou do denominado *jet set*. Diversamente, a informação, patrimonial ou não, passava a ser elemento estruturante da organização de qualquer

[21] "Se este é o quadro global a ser observado, não é mais possível considerar os problemas da privacidade somente pelo pêndulo entre "recolhimento" e "divulgação"; entre o homem prisioneiro de seus segredos e o homem que nada tem a esconder; entre a "casa-fortaleza", que glorifica a privacidade e favorece o egocentrismo, e a "casa-vitrine", que privilegia as trocas sociais; e assim por diante. Essas tendem a ser alternativas cada vez mais abstratas, visto que nelas se reflete uma forma de privacidade que negligencia justamente a necessidade de dilatar esse conceito para além de sua dimensão estritamente individualista, no âmbito do qual sempre este confinado pelas circunstâncias de sua origem" (RODOTÁ, 2008, p. 25),

> poder, público ou privado, que tem nela a ferramenta básica para alcançar a eficiência administrativa ou empresarial e controlar os cidadãos para a gestão de políticas dominantes ou aos comportamentos prevalecentes.

Sendo assim, para defender a privacidade não é suficiente elaborar um sistema para conter o uso dos computadores ou *smartphones*, devendo-se, em verdade, observar seus impactos e distintos significados que possam assumir no conjunto do sistema político e social.

A tutela da privacidade deve ser fundada na proteção e controle do uso de informações pessoais em dados por empresas e governos. Consequentemente, ela deve ser enxergada em um contexto mais amplo, levando em conta as inovações científicas e tecnológicas que a definem como sendo uma ferramenta essencial para o desenvolvimento da personalidade.

Simplificando, a legislação que busca uma efetiva proteção a dados pessoais e a proteção desta "nova dimensão" da privacidade não pode e não deve se pautar pela restrição a serviços e tecnologias. Deve garantir o menor limite possível de manuseamento dos dados pessoais do indivíduo por terceiro sem o conhecimento e anuência do mesmo e buscar assegurar o livre desenvolvimento da personalidade e a participação de maneira autônoma nas vidas política e social por meios digitais.

Nessa esteira, a defesa da privacidade não pode ser possível por meio de uma ação que combata à utilização de tecnologias comuns por todas as organizações sociais modernas.

Sobre o ponto:

> Trata-se de uma tendência determinada por fenômenos interdependentes. Às novas formas de coleta e tratamento de informações, possibilitadas, sobretudo pelo recurso a computadores, adiciona-se a crescente necessidade de dados por instituições públicas e privadas: como não é imaginável uma ação que vá ao encontro a esta tendência, comum a todas as organizações sociais modernas, é necessário considerar de forma realista tal situação, analisando as transformações que causa na distribuição e no uso do poder pelas estruturas públicas e privadas. (RODOTÁ, 2008, p. 24)

Para uma efetiva tutela, torna-se necessário problematizar o uso destas informações e legitimar quem deve ter o controle, uma vez que é praticamente impossível esperar que qualquer Estado ou empresa renuncie a essa estrutura informativa sofisticada. Devem-se considerar as transformações que a circulação de dados causa nas estruturas públicas e privadas. E, "somente assim será possível desfazer o nó das relações entre a tutela das liberdades individuais e a eficiência administrativa e empresarial" (RODOTÁ, 2008, p. 24).

Passa pela análise dos poderes político e econômico que surgem na manipulação dessas informações. Entender o funcionamento deles torna possível não apenas projetar formas de controlar esses poderes, mas também aproveitar as possibilidades ofertadas pela tecnologia da computação a fim de tentar produzir formas distintas de gestão de poder, capazes de oferecer às liberdades individuais possibilidades de expansão que antes eram inimagináveis (RODOTÁ,2008, p. 24),

Uma definição da privacidade como "direito de ser deixado só" perdeu há muito tempo seu valor genérico, ainda que continue a abranger um aspecto essencial do problema e possa (deva) ser aplicada a situações específicas (RODOTÁ, 2008, p. 93). Aliás, a dificuldade que se encontra em definir a privacidade com apenas uma natureza já justifica que ela não possa ser simplesmente um direito a ser concretizado subjetivamente, individualmente.

Na sociedade de informação, tendem a imperar definições funcionais da privacidade que, em diversas legislações, fazem referência à "possibilidade de um sujeito conhecer, controlar, endereçar, interromper o fluxo de informações a ele relacionadas" (RODOTÁ, 2008, p. 93). Assim, "a privacidade deve ser considerada também como o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular" (MULHOLLAND, 2012, p. 03)e a realização plena de sua liberdade existencial.

Essa nova perspectiva é fruto de uma lenta evolução a ser percebida no modo que a ONU enfrentou, pela primeira vez, a questão dos efeitos sociais e políticos dos tratamentos automatizados das informações. "No parágrafo 1, "c", da Resolução 2.450 (XXIII), de 19 de dezembro de 1968, a Assembléia Geral sublinhava os usos da eletrônica que possam incidir sobre os direitos do cidadão e os limites que deveriam ser previstos para tais usos em uma sociedade democrática" (RODOTÁ, 2008, p. 48).

Ecoando esses novos significantes, Gilmar Ferreira Mendes e Paulo Gustavo Gonet Branco (2012, p. 407-408) aduzem que o direito à privacidade tem por objeto os comportamentos e os acontecimentos atinentes às pessoas e às relações comerciais e profissionais que a pessoa não deseja que se espalhem ao conhecimento público. Além disso, os autores supracitados afirmam que "no âmago do direito à privacidade está o controle de informações sobre si mesmo" (2012, p. 410).

Para José Afonso da Silva (2009, p. 206), a privacidade em nossos tempos abarca um conjunto de informações sobre o indivíduo sobre as quais ele pode decidir manter sob seu controle exclusivo ou mesmo comunicar, definindo, ainda, a quem, quando, onde e em condições, sem que seja legalmente sujeito a isso.

Especifica-se, desse modo, privacidade na sociedade de informação como um direito de controle sobre as informações pessoais que atua na construção da esfera privada em sua totalidade e que se apresenta como "precondição da cidadania na era eletrônica e, como tal, não pode ser confiada unicamente à lógica da auto-regulamentação ou das relações contratuais" (RODOTÁ, 2008, p.129). Esse novo entendimento sobre a privacidade necessariamente está atrelada à construção de nossa autoimagem, a ser resguardada pelos nossos direitos da personalidade.

Mas apesar da pertinência do estudo da matéria para uma completa noção da complexidade e abrangência do direito da privacidade na sociedade de informação, esse não é o escopo do presente trabalho. Para o mesmo, importa compreender que a privacidade não é mais uma dimensão de exclusivo sigilo, à margem do tecido social.

Portanto,a proteção da privacidade está umbilicalmente interconectada à proteção de dados pessoais muito embora ambas não se equiparem. Enquanto a proteção da privacidade é atrelada a um controle sobre as informações pessoais, a proteção de dados busca uma guarida mais ampla que envolve reflexões sobre quem manipula essas informações, se podem ser manipuladas, em que condições, com que fins e ainda sobre quais condições foi autorizada essa manipulação.

Porém, antes de se adentrar do estudo específico da proteção de dados, é imperioso fazer um recorte da sociedade de informação brasileira.

2.2 A SOCIEDADE DE INFORMAÇÃO NA REALIDADE BRASILEIRA

Sobre a realidade local, em pesquisa recente sobre o uso de Tecnologias de Informação e Comunicação (TIC), o Comitê Gestor da Internet no Brasil (CGI) demonstra que é cada vez mais comum o uso das tecnologias digitais móveis para o acesso à internet no cotidiano dos brasileiros. Apesar das enormes disparidades entre regiões do país e classes sociais.

Certamente, a exclusão digital é um gargalo ainda proeminente, uma vez que cerca de 50% dos domicílios possuíam algum tipo de acesso à internet. Portanto, cerca de metade da população ainda se encontra sem acesso no domicílio, utilizando-se de outros espaços para conectarem-se, principalmente nas áreas rurais e nas regiões Norte e Nordeste o que exige e demanda ações públicas no quadro.

Contudo, objetivamente existe a tendência progressiva de inclusão e seguramente em estudos futuros mais lares brasileiros estarão conectados, sendo esta a regra.

O que salta aos olhos é a plataforma com maior aderência, o smartphone, no acesso à internet. Talvez pela facilidade de adesão particular e pelo avançar da estrutura de telefonia,no Brasil, em todos os estratos da população, o uso do telefone celular já se tornou o principal dispositivo para o acesso a internetultrapassando o computador.

Entre os usuários da rede, que correspondem a 58% da população com 10 anos ou mais, 89% acessaram a internet pelo telefone celular, enquanto 65% o fizeram por meio de um computador de mesa, portátil ou tablet. E35% dos usuários de internet acessaram a rede apenas pelo telefone celular, sendo especialmente proeminente entre os usuários de classes sociais menos favorecidas e aqueles da área rural.

Esses índices são particularmente relevantes porque apontam o uso das TIC cada vez mais atreladas a tecnologias móveis e, portanto, o uso de aplicativos que, por sua vez, utilizam-se principalmente de dados pessoais. Conforme dados coletados, Chen Wen Hsing e Cesar Alexandre de Souza (2015, p. 75) demonstram que aplicativos móveis que coletam dados pessoais estão cada vez mais comuns no cotidiano do brasileiro.

Nada menos do que 92% da população têm acesso a celulares, sendo que 39% destes usuários regulares baixaram aplicativos nos últimos três meses e, no mínimo, 62% usaram o aparelho para atividades que exigem funcionalidades típicas de smartphones. Essas atividades incluem tirar fotos, ouvir música e aplicativos.

Somente com esses dados já é possível inferir que: a) a maioria da população brasileira já tem acesso à internet; b) dentro desta maioria, é predominante o acesso à internet por plataformas móveis que se utilizam, e muito, de dados pessoais para utilização.

Assim, naturalmente se multiplicam as questões jurídicas que envolvem a violação ou não de nossa privacidade quanto ao monitoramento destas funcionalidades cotidianas com o uso destas tecnologias. Tecnologias que reconstroem pessoas físicas em perfis virtuais utilizados por empresas diversas, muitas vezes semo conhecimento ou consentimento das mesmas, para a melhora de seus serviços e maior efetividade comercial.

Portanto, para Rodotá (2008, p. 25), e corroborado com a pesquisa apresentada pelo CGI, a atual configuração social brasileira impõe questões inerentes ao direito à privacidade atreladas à projeção da personalidade pela divulgação dos dados pessoais e a utilização dos mesmos em atividades cotidianos do novo dia a dia, exigindo do legislador um tratamento pertinente sobre o assunto.

Em relação às informações pessoais, a legislação brasileira ainda adota uma postura “paternalista”, preocupada em impedir a ofensa à privacidade e ao mau uso de dados pessoais. Neste sentido,

> Parece relevante assinalar que, ao proceder às necessárias ponderações, se deve atentar para a armadilha de uma tutela "paternalista". Ordenamentos de tipo paternalista só são compatíveis com sociedades infantilizadas, tidas como irresponsáveis, ignorantes e inconsequentes, às quais em regra tudo deve ser proibido, ou regulado, podendo-se fazer apenas o que é expressamente permitido – princípio este que é próprio dos sistemas fascistas e, portanto, incompatível com sistemas democráticos. 33 Ao paternalismo, contido na máxima segundo a qual "as pessoas devem ser protegidas de si próprias", deve ser oposta a presunção que vigora nas sociedades democráticas: a liberdade de escolha acerca do próprio destino não pode ser exceção. ((MORAES, 2010, p.10)

Desse modo, a tutela dos dados pessoais, uma garantia do exercício de direito à privacidade, ainda é insipiente no Brasil, apesar da demanda jurídica demonstrada

Tal quadro exige uma correta análise da realidade e a construção de sistemas jurídicos realmente eficazes quanto à proteção dos dados pessoais, inclusive enxergando nessa guarida um exercício da dignidade humana.

3. A PROTEÇÃO DE DADOS COMO UM DIREITO FUNDAMENTAL

As proposituras de legislação atuais sobre proteção de dados visam justamente à superação do direito à privacidade apenas como um direito de ser deixado só. Ancora-se em uma visão de privacidade que garante o controle pelos indivíduos sobre o uso de seus dados e informações pessoais a partir das inovações trazidas pela internet[22].

É o que se enxerga com clareza em legislações sobre a *informal privacy* nos Estados Unidos, que abordam o acesso a dados pessoais em órgãos públicos, até o estabelecimento da "autodeterminação informativa" pela Diretiva 95/46/CE de 1995 da União Européia.

Apesar de estes textos normativos tratarem do direito a privacidade, o posicionamento das mesmas é de compreender que a proteção de dados não é uma dimensão menor da privacidade. Isto porque propõem o tema da privacidade, mas modificam seus elementos aprofundando os postulados sobre dados pessoais, construindo um arcabouço jurídico específico, com princípios e conceitos próprios.

Em seu aspecto informacional, a privacidade desempenha funções essenciais tanto para o indivíduo como para a sociedade como "a garantia de tolerância e da liberdade de opinião, de associação e de religião; a garantia da livre pesquisa científica; a garantia da lisura do próprio processo eleitoral, e tantos outros quanto possamos descrever" (DONEDA, 2006, p.205).Mas a proteção de dados deve ir além.

Sob o a tutela da proteção de dados pessoais, essas garantias passam a ser vistas por um prisma mais abrangente. Tanto o interesse de quem manipula os dados como dos proprietários são considerados, bem como a forma que esses dados são coletados e armazenados. Busca-se assim compreender as "diversas formas de controle tornadas possíveis com a manipulação de dados pessoais" (DONEDA, 2006, p.204).

O direito à proteção de dados contempla a autodeterminação informativa que herdou da privacidade na sociedade de informação, mas não é um direito subalterno a nenhum outro, inclusive à própria privacidade. Para tanto, segundo Rodotá (2008, p. 18)

> O direito à proteção de dados não deve ser considerado subordinado a nenhum direito. Significa que devemos ir além de uma simples análise balanceada de fatores, porque a própria proteção de dados éum direito fundamental.

[22]"Isto não significa dizer, no entanto, que a tutela que se confere aos dados pessoais será segmentada e valorada de acordo com as informações neles contidas. Diversamente, a proteção aos dados pessoais é única e encontra-se lastreada na tutela integral da pessoa, cuja disciplina é que fornecerá os subsídios necessários para modular o grau de proteção exigido" (BUCAR, 2016, p.709).

Portanto a proteção de dados como um direito fundamental necessita de guarida constitucional específica e legislação ordinária sobre a sua aplicabilidade.

Na realidade, a proteção de dados funciona como um "protetor" ou "garantidor" do exercício da privacidade, da dignidade e dos direitos da personalidade do indivíduo inserido na sociedade de informação,da autodeterminação informativa e da qualidade de como os dados são tratados.

Ainda, a proteção de dados não se resume à "autodeterminação informativa". Apesar de não ser equivocada, essa terminologia não é a mais adequada para a construção de legislação específica sobre os dados pessoais no contexto brasileiro. A expressão "direito à proteção de dados" é preferível sobre "autodeterminação informacional" por englobar todos os rótulos e conceitos de maneira mais ampla. É inclusive por isso recepcionada com mais amplitude pelas normas internacionais sobre a matéria que hodiernamente reconhecem o direito à proteção de dados como um direito fundamental (DONEDA, 2006, p. 201).

Ao se integrar essa multiplicidade de setores e sujeitos participativos, a construção legislativa se torna horizontal. Ao mesmo tempo, com possibilidades maiores de se convergirem em diversas partes do mundo, uma vez que os participantes muitas vezes possuem natureza transacional[23].

Talvez isso ocorra porque os países pioneiros em normas sobre a proteção de dados,especificamente do bloco europeu e EUA, sejam aqueles que a economia de informação já está implementada há certo tempo. Nesses países o uso da informação como recurso de base nos processos produtivos, comerciais e na própria sociedade é resultado direto do desenvolvimento tecnológico da informática e da computação. Não por menos, a proteção de dados como direito fundamental já é claramente abordada com uma teoria e, inclusive, como um ramo específico do Direito[24].

Evidentemente, tais paradigmas e fundamentos surgiram e evoluíram conforme a tecnologia avançava. Desde um prisma mais restrito, técnico e centralizado pelo Estado até as atuais legislações que compreendem a natureza descentralizada, cooperativa e dinâmica da

[23]"Instauram-se relações entre pares, a construção torna-se horizontal. No curso deste processo, será possível conseguir resultados parciais, a integração entre códigos de autorregulação e outras formas de disciplina; normativas comuns para áreas únicas do mundo, como demonstra novamente a União Europeia, a região do mundo onde é mais intensa a tutela desses direitos e, como se poderia esperar, para matérias onde já foi atingida uma maturidade cultural e institucional, como aquela relativa à proteção dos dados pessoais" (RODOTÁ, 2015, p. 03).

[24]"A autonomia da temática da proteção de dados pessoais é uma tendência hoje fortemente enraizada em diversos ordenamentos jurídicos. O desenvolvimento autônomo desta matéria foi intenso nas mais de quatro décadas que a disciplina ostenta, desde as primeiras formulações no final da década de 1960, quando a utilização de dados pessoais começou a ser um tema debatido pela sociedade a partir do desenvolvimento tecnológico e da constatação de que seus efeitos para a sociedade seriam notáveis" (DONEDA, 2015, p.370).

informação pelo advento da computação na internet.Passaremos, então, a uma análise breve dos principais fundamentos da matéria.

3.1 ATEORIA DA PROTEÇÃO DE DADOS

Coma sociedade de informação já em escala global, o discurso sobre a privacidade concentrou-se cada vez mais em questões relacionadas à proteção de dados. Neste sentido, entender em que ponto os "dados pessoais" integram-se como parte da informação torna-se urgente.

A utilização dos termos "dados" ou "informações" de forma indistinta é comum ao meio jurídico[25]. Porém, apesar de ambos representarem um fato ou característica de uma realidade ou de alguém, cada qual possui uma "carga" própria a se levar em conta.

Dessa forma, o "dado", enxergado de maneira mais restrita o possível, seria uma informação ou fragmento de informação em estado potencial, pré-transmitida ou como uma "pré-informação" anterior à coleta, interpretação ou processamento por uma tecnologia

Já a informação estaria mais ligada à cognição que transmite sobre quem ou aquilo que representa, chegando a interferir no receptor sob seus efeitos. Ainda, a informação estaria inexoravelmente vinculada a determinados valores em que estão representadas. Isso explica doutrinas clássicas sobre liberdade de informação ou no dever de informação ao consumidor.

Deste modo a carga semântica de dado é distinta da de informação. A primeira explora uma potencialidade, uma possibilidade de ser uma informação conhecida. Já a segunda só se consubstancia quando o receptor tem acesso a ela (DONEDA, 2006, p. 152).

Também sobre o tema, o Conselho Europeu, por meio da Convenção de Strasbourg, de 1981, ofereceu uma definição que condiz com essa ordem conceitual. Nela, informação pessoal é "qualquer informação relativa a uma pessoa singular identificada ou susceptível de identificação"(DONEDA, 2006, p. 152).

Assim, ao contrário do dado, a informação independe de qualquer meio para se propagar ou ser comunicada, sendo um produto autônomo e anterior a todos os serviços dos quais é objeto. Ainda, as informações possuem naturezas diversas, desde relativas às pessoas, às opiniões subjetivas, aos patrimônios, dentre tantas outras.

---

[25]"Parte da doutrina aponta a inexistência de diferença semântica entre dado pessoal e informação pessoal, afirmando serem ambos os termos sinônimos. É inquestionável que ambos representam de alguma forma, uma característica peculiar, ainda que fragmentada, relacionada à determinada pessoa. São, portanto, reflexo da realidade pessoal" (BUCAR, 2016, p.663).

Em relação à conceituação de dado Bucar (2016, p.699) resgata definição apresentada pelo artigo 2º da Diretiva Européia 95/46/CE [26] relativa ao tratamento e à circulação de dados pessoais:

> Para efeitos da presente diretiva, entende-se por dados pessoais qualquer informação relativa a uma pessoa singular identificada ou identificável ("pessoa em causa"); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social.

Tal distinção torna-se relevante para destacar o seguinte entendimento: o que diferencia a informação hoje na sociedade de informação dos seus moldes tradicionais é a capacidade de manipulação, armazenamento e coleta organizada – ou explicitando, sua conversão em dados digitais – proporcionada pela computação.

As ditas "informações pessoais", ou aquelas que possuem um vínculo objetivo com uma pessoa[27]. Já o "dado pessoal", pode manter vínculos com a pessoa e ainda assim ser anônimo, demonstrando utilidades diversas quando analisados na coletividade ou em grupos distintos de pessoas[28].

Ainda, essa distinção também serve como alicerce a conceitos importantes nas legislações sobre dados pessoais, como os de "dados sensíveis". Eles seriam determinadas informações que, caso sejam conhecidas ou processadas, prestar-se-iam a uma potencial utilização discriminatória ou particularmente lesiva a determinadas pessoas ou coletividades. Esses seriam dados pessoais sobre credo, raça, opção sexual, histórico médico ou dados genéticos de um indivíduo (BUCAR, 2016, p.722).

Mas apesar dessa distinção semântica, usualmente dados pessoais são reconhecidos como informações, ou partes de informações, que podem ou são submetidas a algum

---

[26] Artigo 2º da Diretiva 95/46/CE, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (União Européia. Diretiva 95/46/CE. Disponível em: <http://www.abdi.org.br/upload/dir1995-46_en.pdf>. Acesso em: 09 de fevereiro de 2017.

[27] "Este vínculo significa que a informação refere-se às características ou ações desta pessoa, que podem ser atribuídas em conformidade com a lei, como no caso do nome civil ou do domicílio, ou então, às informações provenientes de seus atos, como os dados referentes ao seu consumo, informações provenientes de suas manifestações, como as opiniões que manifesta, e tantas outras" (DONEDA, 2006, p. 156).

[28] "Esta chamada anonimação de dados pessoais – a retirada do vínculo da informação com a pessoa a qual se refere – é um recurso que algumas leis de proteção utilizam para reduzir os riscos presentes no seu tratamento, o que é realizado em menor escala, também com a utilização de pseudônimos. O Dado anônimo ainda pode apresentar útil em outras hipóteses, como aquela na qual possibilita a comunicação e expressão de sujeitos que estariam impedidos, por vínculos e limitações políticas ou sociais, de exprimir-se livremente" (DONEDA, 2006, p. 157).

tratamento tecnológico. Corroborando essa observação, Antônio Espíndola Longoni e Guilherme Magalhães Martins (2015, p. 291)afirmam que:

> A expressão "dados" é a tradução da palavra latina e também inglesa *data*, significando "informações". Usualmente, dados são informações. Tecnicamente, são informações que passam por algum tipo de tratamento, ainda que simples coleta, por meio eletrônico ou não. Dessa forma, sigilo de dados significa sigilo de informações tratadas, de forma informatizada ou não. E mais: é o sigilo de qualquer caráter nominativo, possibilitando identificar direta ou indiretamente a pessoa referida. A inviolabilidade é conferida com relação à utilização desleal das informações.

Portanto, a proteção de dados pessoais busca proteger informações pessoais em estado potencial, antes durante e depois do tratamento das mesmas pela tecnologia. Entre uma noção de "informação base" disponibilizada por um indivíduo e uma "informação resultados" obtida de um tratamento específico em busca de uma utilidade qualquer, por exemplo, estatístico ou comercial. Ou, conforme Doneda (2006, p.181)

> Os dados pessoais passam a ser os intermediários entre a pessoa e a sociedade, prepostos nem sempre autorizados e capazes, e é justamente isto que produz como efeito a perda de controle da pessoa sobre o que se sabe em relação a si mesma- o que, em última análise, representa uma diminuição na sua própria liberdade.

A informatização proporcionou ao tratamento desses dados melhoras qualitativas e quantitativas. As melhoras qualitativas referente às novas tecnologias como algoritmos, *profiling*[29], *data mining*[30] *ou data maching*[31], enquanto que as quantitativas são referentes à massificação do poder de processamento e demaneiras de obtenção de nos tipo de utilidades.

---

[29]"Dentre estas técnicas está a elaboração de perfis de comportamento de uma pessoa a partir de informações que ela disponibiliza ou que são colhidas. Esta técnica conhecida como *profiling*, pode ser aplicada a indivíduos bem como estendida a grupos. Nela os dados são tratados , com o auxílio de método estatístico, técnicas de inteligência artificial e outras mais, com o fim de obter metainformação, que consistiria numa síntese de hábitos, preferências pessoas e outros registros da vida desta pessoa" (DONEDA, 2008, p.173).

[30] "Outra técnica ainda diz respeito a uma modalidade de coleta de dados pessoais, conhecida como *data mining*. Ela consiste na busca de correlações, recorrências, formas, tendências e padrões significativos a partir de quantidades muito grandes de dados com o auxílio de instrumentos estatísticos e matemáticos. Assim, a partir de uma grande quantidade de informações em estado bruto e não classificada, podem ser identificadas informações de potencial interesse" (DONEDA, 2008, p.176).

[31] "Outra ferramenta notabilizada pelos poderosíssimos riscos oferecidos à privacidade é o *data matching*: as informações depositadas em dois ou mais bancos de dados de qualquer gênero são cruzadas e emparelhadas formando um novo banco de dados capaz de possibilitar maior aproximação das características e aspectos comportamentais da pessoa. Se esse cruzamento tiver como objetivo apenas confirmar a correção de dados depositados em arquivos diversos, não há como se enxergar qualquer lesão à privacidade. No entanto, se o emparelhamento buscar agregar novos dados – o que usualmente ocorre –, a operação do *data matching* deve ser previamente comunicada ao interessado, seja para que ele tenha conhecimento do espaço em que seus dados circularão, seja para que ele possa controlar e/ou evitar os possíveis resultados eventualmente lesivos que a aplicação dessa tecnologia possa ocasionar. Mas se o cruzamento de informações ocorrer após o depósito de informações pelo interessado, seu consentimento posterior deve ser necessariamente requerido se da aplicação

Sensivelmente essas melhoras quantitativas ou qualitativas no tratamento dos dados apresentam implicações claras sobre as informações pessoais e a privacidade, conforme explana Bucar (2016, p. 924):

> A aplicação dessas técnicas, como se pode perceber, acaba por desmitificar a máxima de que "uma imagem vale mais que mil palavras"; na realidade, com alguns poucos dados, é possível alcançar detalhes da pessoa que revelam muito mais do que sua própria projeção física. Diante desta constatação, uma proteção eficaz de dados pessoais reclama uma articulação de princípios próprios para a tutela da pessoa, visto que bancos de dados constituem uma realidade tanto para o mercado como para a administração pública.

Por lógica, basta pensarmos que se aumentamos ou melhoramos o processamento de dados, necessariamente serão cada vez mais disponibilizadas informações sobre as pessoas, que em meios normais seriam descartadas ou não sofreriam tratamento. Informações essas que determinam seu exercício de personalidade sensivelmente, uma vez que boa parte destas informações esta além do conhecimento ou controle direto.

E o controle dessa dispersão de informações pessoais se torna mais difícil – exigindo o esforço legislativo além do hermenêutico com a criação de novas regulamentações específicas para a proteção de dados pessoais na internet – devido a não dependência de centros específicos de controle e distribuição desta informação.

Isso significa que a internet por natureza é um sistema difuso de distribuição de informações, o que dificulta o esforço em seu controle a partir de uma legislação que regulasse a "base" ou "centralidade"física destes tratamentos.

De certo modo, essa dificuldade foi justamente o evoluir tecnológico da própria internet. Que se desenhou no fracionamento dos grandes centros de processamento de dados – na esmagadora maioria pública ou de grandes corporações industriais – para a utilização em centros médios e pequenos chegando, nos dias atuais, à possibilidade de centros de processamentos caseiros que possuem efetivo desempenho.

Assim, é extremamente precária e incipiente qualquer tentativa de controle de tráfego de dados por bases exclusivamente territoriais. A internet se constitui basicamente em um protocolo de comunicações em computadores, possibilitando sua interligação através dos vários meios de comunicação de dados existentes. "Esta estrutura de rede é capaz de prescindir de "caminhos únicos" – podendo substituir as eventuais vias de comunicação

---

do *datamatching* resultar a obtenção de informação tendente a ensejar postura social discriminatória ou controladora de sua liberdade" (BUCAR, 2016,p.919).

bloqueadas por outras - e como consequência não haveria mais elementos essenciais para seu funcionamento" (DONEDA, 2006, p. 59).

Essa dispersão territorial também impõe uma necessidade da regulação de proteção de dados pessoais em amplitudes globais, não mais sendo de interesse exclusivo dos países desenvolvidos. Ela já se tornou realidade em grande parte do globo, com mais de 101 países com legislações próprias, conforme lembra Doneda (2015, p.370).

Assim, a doutrina sobre a matéria foi evoluindo juntamente com a própria internet e seu uso, se construindo basicamente em quatro diferentes gerações de leis[32], começando com um enfoque estritamente técnico e territorial e ampliando-se conforme a evolução tecnológica da rede.

3.2 AS GERAÇÕES DA PROTEÇÃO DE DADOS

Já é fato notório que o surgimento da internet alargou ostensivamente as possibilidades de comunicação.Tornou a circulação de informação temporalmente imediata e espacialmente relativa, levantando diuturnamente questões difíceis e complexas acerca do manejo das informações pessoais das pessoas. Porém, esta reflexão trazida por uma inovação tecnológica não é inédita, ocorrendo no surgimento do telefone, do rádio ou da televisão, que guardam em comum a ruptura das distâncias e exponencialmente aumentando a interação entre pessoas.

Justamente pela percepção de que estas novas utilizações de informações advindas da tecnologia criaram repercussões sobre diversos direitos personalíssimos, surgiram, em contrapartida, demandas almejando contrabalancear essa tendência.

O paradigma inicial de legislações sobre proteção de dados surgiu a partir de meados da década de 1970, coincidindo com o início da computação pessoal e o surgimento dos grandes "*Data Centers"*. Amadureceu-se em diversos países a tendência de normativas pararegular esses bancos, buscando garantir as liberdades individuais (credo, livre manifestação, sexualidade etc.) e tantas outras demandas surgidas principalmente com o surgimento da rede de computação.

A primeira geração destas leis, como a Lei do *Land* alemão de Hesse de 1970 e o *Privacy Act* norte americano de 1974 buscavam principalmente regulamentar as atividades dos *National Data Centers* e similares, e abordavam as atividades na coleta e gestão dos

[32] Tal classificação geracional e evolutiva foi realizada por Viktor Mayer- Sconberger em seu artigo "*General developmente of data protection in Europe*" presente na obra "*Tecnology and privacy: the new landscape*" de 1997 (DONEDA, 2008, p.209).

dados pessoais pelo Estado e órgãos públicos. Refletiam fundamentalmente a tentativa, feita pelos Estados, de regular a concessão de autorizações para a criação desses bancos de dados e do seu controle *a posteriori*(DONEDA, 2015, p. 373).

Portanto, essas legislações pautavam-se no controle do uso das informações pessoais pelos Estados em todos os seus entes e estruturas administrativas, como os destinatários principais destas normas. São regramentos que demonstram uma tentativa inicial de regulamentação estatal sobre dados pessoais, contra um uso indiscriminado dessa tecnologia, mas sem que se soubessem ao certo suas conseqüências.

Devido ao desconhecimento da tecnologia e sua aplicabilidade, essas leis optavam por "princípios de proteção, não raro bastante abstratos e amplos, focalizados basicamente na atividade de processamento de dados, além de regras concretas e específicas dirigidas aos agentes diretamente responsáveis pelo processamento dos dados" (DONEDA, 2015, p. 371).

O prisma, portanto era conter um uso danoso da tecnologia, especificamente relacionada a computadores e redes. A estrutura e a gramática de tais leis era algo tecnocrático e condicionado pela informática, pois tratavam dos "bancos de dados", e não propriamente da "privacidade", desde seus princípios genéricos até os regimes de autorização e de modalidades de tratamento de dados (DONEDA, 2015, p. 371).

Essa primeira geração de leis se tornou ineficaz com celeridade diante do avançar da computação doméstica e a multiplicação exponencial dos centros pequenos de processamento de dados, inviabilizando qualquer controle ou monitoramento pelo Estado. Essa geração termina com o surgimento da *Bundesdatenschutzgesetz*, a lei federal da República Federativa da Alemanha sobre proteção de dados pessoais, de 1977[33].

Já a segunda geração tinha em conta justamente a dispersão dos bancos de dados informatizados e das centrais de processamento. Segundo Doneda (2011, p.97) "os primeiros exemplos foram Lei Francesa de Proteção de Dados Pessoais de 1978, intitulada *Informatique et Libertées*, além da já mencionada *Bundesdatenschutzgesetz*".

A principal e diferencial característica desta geração em relação à anterior é que o foco não mais é nos bancos de dados ou nas estruturas físicas da computação e seu uso pelos entes governamentais, mas finalmente considerando a privacidade e a proteção dos dados perante os usuários, funcionando como garantias de liberdade negativa para os mesmos.

[33]A República Federal da Alemanha despontou como pioneira ao legislar sobre proteção de dados pessoais, primeiramente com a Lei do *Land*, de 1970, e em posterior sentença jurisdicional, a *Bundesdantechutzgestz*, de 1977, sobre a competência da coleta de dados pessoais da população questionando e tencionando a "fome" estatal sobre os dados pessoais.

Funcionavam como um arcabouço jurídico que garantia ao próprio cidadão a busca da tutela estatal em casos que suas liberdades fossem vilipendiadas por terceiros. Mas essas leis não se adequavam ao paradigma tecnológico que mudava aceleradamente exigindo cada vez mais o fornecimento de dados pessoais para a participação da vida em sociedade(DONEDA, 2015, p. 373).

Isto porque, tanto o Estado como os entes privados passaram a utilizar intensamente o fluxo de informações pessoais para seu funcionamento, criando uma questão de demanda de dados não apreciada pelas leis[34].

Como cabia ao cidadão exercer o direito de coibir ou parar esta utilização,quando o mesmo buscava interromper ou investigar a pretensa violação de seus dados, implicava-se necessariamente na exclusão dos mesmos, o que afetava a sua participação naquela atividade social (DONEDA, 2011, p. 97).

Na terceira geração, surgida principalmente na década de 1980, a proteção de dados pessoais aprimorou-se ainda que centrada no cidadão como a geração anterior. O salto se deu resolvendo a questão de não apenas garantir as liberdades negativas, mas assumir um caráter positivo de efetivação dos direitos do cidadão na proteção de dados pelo Estado[35].

Surge o direito a "*autodeterminação informativa"* que aparece com a extensão das liberdades negativas da segunda geração para um papel mais pró-ativo na proteção dos dados pessoais. A partir destas leis, a proteção de dados pessoais era "como um processo, que não se encerrava na simples permissão ou não da pessoa à utilização de seus dados pessoais, porém procurava incluí-la em fases sucessivas do processo" (DONEDA, 2015, p.373).

O marco normativo destas leis da terceira geração na realidade é a decisão proferida pelo Tribunal Constitucional Alemão sobre a *Bundesdatenschutzgesetz*, da década de 1970, e legislações regionais dos *Lander* sobre a coleta de dados pessoais da população com a "superioridade" dos direitos à autodeterminação informacional do cidadão contra a "sanha" catalográfica dos estados em mapear a população. Destaca Doneda (2006, p.211):

---

[34]"Estas leis apresentavam igualmente seus problemas, o que motivou uma subsequente mudança de paradigma: percebeu-se que o fornecimento de dados pessoais pelos cidadãos tinha se tornado um requisito indispensável para a sua efetiva participação na vida social. O que era exceção veio a se tornar regra. Tanto o Estado quanto os entes privados utilizavam intensamente o fluxo de informações pessoais para seu funcionamento, e a interrupção ou mesmo o questionamento deste fluxo pelo cidadão implica muito frequentemente a sua exclusão de algum aspecto da vida social" (DONEDA, 2011, p.98).

[35]"A proteção de dados é vista, por tais leis, como um processo mais complexo, que envolve a própria participação do indivíduo na sociedade e considera o contexto no qual lhe é solicita- do que revele seus dados, estabelecendo meios de proteção para as ocasiões em que sua liberdade de decidir livremente é cerceada por eventuais condicionantes – proporcionando o efetivo exercício da autodeterminação informativa" (DONEDA, 2015, p.373).

> Estas leis refletem a proliferação dos bancos de dados interligados em rede e a crescente dificuldade em localizar fisicamente o armazenamento e a transmissão dos dados pessoais. O marco destas leis de terceira geração é a decisão do Tribunal Constitucional Alemão, que mencionamos anteriormente, à qual se seguiram emendas às leis de proteção de dados na Alemanha e na Áustria, além de leis específicas nas Noruega e na Finlândia.

Estas leis também tratavam de garantias como o direito à informação sobre os dados e os processos adotados por terceiro, mas o acesso para a população não era garantido ou facilitado. Neste arcabouço, a "autodeterminação era privilégio de poucos, que custeavam os caros encargos econômicos e sociais dos exercícios destas prerrogativas" (DONEDA, 2011, p.98), o que mitigava a tutela da proteção de dados a setores muitos específicos que utilizavam intensamente a computação.

Buscando suplantar esse caráter elitista e exclusivista, surgiu uma quarta geração de leis sobre proteção de dados pessoais como as que existem hoje. Que visam popularizar o controle sobre dados pessoais e coíbe o enfoque individualista da terceira geração e tutela o uso dos dados pessoais do cidadão comum.

Nessas leis, procura-se enfocar o problema integral da informação, pois elas presumem que não se pode basear a tutela dos dados pessoais simplesmente na escolha individual, mas enfrentar o problema integral da informação na escolha de padrões coletivos do tratamento de dados.

Estas legislações almejam ainda a afirmação e efetivação de um modelo de autoridades independentes para a tutela da lei, como órgãos públicos e entidades privadas que se empenhem na criação de normas específicas para alguns setores de processamento de dados como saúde, comércio, crédito ou consumo (DONEDA, 2015, p.374).

Conforme se exprime, no avançar das gerações sobre a proteção de dados pessoais apresentou-se um desenvolvimento quase que espelhado ao da própria informática, a saber, de nichos estatais e concentrados para o uso disperso e difuso do usuário.

3.3PRINCÍPIOS DA PROTEÇÃO DE DADOS

Certamente a escolha de princípios pertinentes à proteção dados pessoais varia conforme o tempo e a disposição geográfica que atenderia às particularidades do sistema jurídico e político de cada nação. Em sua obra Rodotá (2008, p.59) buscou, em reflexão sobre

a atividade legislativa de mais de trinta anos na Europa sobre proteção de dados, construírem o que denominou de "núcleo comum" da disciplina jurídica da proteção de dados.

Para tanto, concluiu que este núcleo surgira de pontos em comum da Convenção do Conselho da Europa de 28 de Janeiro de 1981 com a Recomendação da OCDE de 23 de setembro de 1980[36]. Diversos princípios são deduzíveis, conforme assinala Rodotá (2008, p.59):

> *1.princípio da correção* na coleta e no tratamento das informações;
> *2. princípio da exatidão* dos dados coletados, acompanhados pela obrigação de atualização;
> *3. princípio da finalidade* da coleta de dados, que deve poder ser conhecida antes que ocorra a coleta, e que se especifica na relação entre dados colhidos e a finalidade perseguida (*princípio da pertinência*); na relação entre finalidade da coleta e a utilização dos dados (*princípio da utilização não-abusiva*); na eliminação, ou transformação em dados anônimos das informações que não são mais necessárias (*princípio do direito ao esquecimento*);
> *4. princípio da publicidade* dos bancos de dados que tratam as informações pessoais, sobre os quais deve existir um registro público;
> *5. princípio do acesso individual*, com a finalidade de conhecer quais são as informações coletadas sobre si próprio, obter a sua cópia, obter a correção daquelas erradas, a integração daquelas incompletas, a eliminação daquelas coletadas ilegitimamente;
> *6. princípio da segurança* física e lógica da coleta dos dados.

Corroborando este posicionamento, Doneda(2015, p.376) acrescenta que na realidade esse núcleo de princípios também apareceu a partir de trabalhos realizados na secretaria americana de saúde, educação e bem estar social.

Esses princípios surgiriam com a "*Records computers and the rigths of citizens"*[37], que buscara uma garantia dos dados pessoais do cidadão a partir da seguinte descrição traduzida por Doneda (2005, p.215):

> -Não deve existir um sistema de armazenamento de informações pessoais cuja existência seja mantida em segredo.
> - Deve existir um meio para um indivíduo descobrir quais informações a seu respeito estão contidas em um registro e de que forma ela é utilizada.

---

[36] Seguindo o mesmo entendimento Bucar (2016, p. 232) afirma que: "Organização para Cooperação e Desenvolvimento - OCDE, entidade que congrega 30 países que produzem a metade da riqueza do mundo (incluindo Estados Unidos e os países da Europa Ocidental), editou, em 1980, uma série de recomendações (guidelines) acerca da proteção da privacidade e do fluxo de dados pessoais. Neste documento, estão previstas essas medidas acautelatórias (Organization for EconomicCo-OperationandDevelopment. OECD guidelines on the protection of privacy and transborder flows of personal data). Disponível em: <http://www.oecd.org/document/18/0,2340,es_2649_34255_1815186_1_1_1_1,00.html>. Acesso em: 10 mar. 2008)".

[37] E.U.A., *Records, computerss and the rigths of citizens. Report of the Secretary's Advisory Comittee on Automated Personal Data Systems*, 1973.Disponível em: <https://www.justice.gov/opcl/docs/rec-com-rights.pdf>. Acesso em :13 de fevereiro de 2017.

> - Deve existir um meio para um indivíduo evitar que a informação a seu respeito coletada para um determinado propósito não seja utilizada ou disponibilizada para outros propósitos sem o seu consentimento.
> - Deve existir um meio para um individuo corrigir ou retificar um registro de informações a seu respeito.
> -Toda organização que crie, mantenha, utilize ou divulgue registros com dados pessoais deve garantir a confiabilidade destes dados para fins pretendidos e deve tomar as devidas precauções para evitar o mau uso destes dados.

Assim, apresenta-se a mesma síntese de princípios, com algumas pequenas distinções de terminologia: *transparência* ao invés de *publicidade*; *qualidade* ao invés de *correção e exatidão*; *livre acesso* ao invés de *acesso individual* e subdividindo o princípio da *finalidade* em *proporcionalidade* e *necessidade* (DONEDA, 2015, p.377*).*

De toda forma, sendo os seis princípios apontados por Rodotá ou os sete apontados por Doneda, é certo afirmar que foi esse "núcleo comum" que forma a espinha dorsal da grande maioria de legislações pertinentes na Europa e que servem ainda de inspiração aos especialistas nacionais brasileiros. Inclusive, serve de fundamentação ao PL nº 5276/2016 de autoria do Poder Executivo e em tramitação na Câmara dos Deputados, no qual Doneda participou da elaboração.

O *princípio da transparência* (ou *publicidade*) informa que todo e qualquer banco de dados pessoais deve ser de conhecimento público, bem como as modalidades e tecnologias ou técnicas adotadas na coleta e utilização das informações pessoais pelo mesmo (RODOTÁ, 2008, p.59). Se aposta na influência e no poder da opinião publica como mecanismo de controle eficaz sobre a utilização dos dados, indo além da mera guarida estatal. A publicidade então funciona inclusive como um princípio de fomento à autodeterminação informativa, uma vez que "educa" os usuários a se informarem sobre quem e como seus dados são tratados.

O *princípio da qualidade* informa que os dados armazenados necessariamente devem se atinar à realidade, exigindo da coleta e tratamento dos dados correção e cuidado e atualizações frequentes. Esse princípio é de extrema relevância no contexto atual da chamada *pós-verdade*[38] e de redes sociais.

Tanto Rodotá (2008, p. 59) quanto Bucar (2016, p. 946) abordam no princípio da exatidão (que é equivalente à qualidade) a necessária exatidão dos dados armazenados e a

[38] De acordo com o *Oxford Dictionaries*, a pós-verdade ou "*post-truth*", é uma adjetivação que"se relaciona ou denota circunstâncias nas quais fatos objetivos têm menos influência em moldar a opinião pública do que apelos à emoção e a crenças pessoais", ou seja, a alteração da maneira de se observar fatos buscando fins específicos a partir da manipulação subjetiva da população.Mais detalhes disponíveis em:<https://www.nexojornal.com.br/expresso/2016/11/16/O-que-%C3%A9-%E2%80%98p%C3%B3s-verdade%E2%80%99-a-palavra-do-ano-segundo-a-Universidade-de-Oxford>. Acesso:13 de fevereiro de 2017.

preocupação de que os mesmos reflitam a realidade fática que retratam, exigindo dos bancos de dados atenção a essa veracidade.

Já o *princípio da finalidade* exige que o usuário saiba antes a qual utilidade o uso de seus dados vai receber. Segundo Doneda (2015, p.376), é neste principio que se fundamenta "a restrição da transferência de dados pessoais a terceiros, além do que se pode, a partir dele, estrutura-se um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade (fora do qual haveria abusividade)".

De acordo com esse princípio o motivo da coleta ou utilização do dado deve ser compatível com qual tratamento ele irá receber, criando uma ligação direta entre a informação e sua origem, no caso a pessoa. É o princípio que fundamenta o consentimento informado.

O *princípio do livre acesso* informa que cada indivíduo deve ter acesso pleno aos seus dados no banco de dados onde estão armazenadas, seja para conhecer quais são as informações pessoais contidas nestes dados ou para obter cópias destes, com o devido controle para fins de correção, supressão ou eventuais acréscimos (BUCAR, 2016, p.938).

Sobre o mesmo é evidente sua ligação com a ideia da autodeterminação informativa surgida na segunda geração de leis de proteção de dados, ao garantir ao indivíduo o controle de que as informações representadas nos dados condizem com a realidade fática.

Já o *princípio da segurança física e lógica* aborda a necessária prevenção por quem manipula dados pessoais em resguardá-los contra riscos de extravio, destruição, transmissão ou acesso não autorizado (BUCAR, 2016, p.951).

Esse princípio é talvez um dos que justifiquem a necessidade de uma guarida especial à proteção de dados. Afinal, a proteção da privacidade em uma dimensão de autodeterminação informativa não se ocupa de problematizar as condições físicas dos tratamentos de dados. É uma prova cabal que a proteção de dados é uma disciplina distinta.

O *princípio da proporcionalidade* exige que os dados pessoais somente possam ser tratados se relevantes à finalidade previamente anunciada pelo qual foram coletados, evitando a abusividade na utilização destes dados. Segundo Doneda (2015, p.377) sobre o princípio em questão "em algumas legislações, este princípio é reforçado pelo princípio da necessidade, pelo qual somente podem ser utilizados dados pessoais caso a finalidade almejada não posso ser atingida de outro modo".

E finalmente, *o princípio da necessidade* determina que "devem ser coletados e tratados somente os dados pessoais que são necessários para o atendimento de uma determinada finalidade, descartando-se os dados exorbitantes" (DONEDA, 2015, p.377).

Destarte, desse rol de princípios é possível perceber que os mesmos possuem a instrumentalidade necessária para a efetivação dos objetivos almejados tanto pela *Records computers and the rigths of citizens,* como pela grande maioria das legislações nacionais e transacionais sobre o tema.

Em conformidade com as prerrogativas da quarta geração de legislações sobre proteção de dados pessoais, verifica-se que a adoção desse núcleo comum de princípios permite uma mudança do perfil passivo do usuário para um caminho mais pró-ativo.

Ainda, uma virada hermenêutica da legislação que se ocupa apenas em tutelar e coibir os abusos para uma legislação mais positiva e dinâmica que se ocupa de todo o processo de manipulação de dados, antes da coleta até a sua utilização.

Deste modo, as legislações[39]vêem se construindo com uma tendência à autonomia da proteção de dados como matéria especifica e independente da privacidade, alçando inclusive como um direito fundamental em diversos ordenamentos (DONEDA, 2015, p. 378).

Portanto, antes de adentrarmos especificamente no regime jurídico de proteção de dados existente no Brasil atualmente, e sua eventual análise, é importante apresentar um exemplo de aplicação legislativa adequada à matéria.

Em panorama geral facilmente poderia se analisar no contexto internacional a *US Fair Information Principles* de 1973 (com aplicação até hoje) ou a *US – EU Privacy Shield* que funciona como um tratado de dados entre Europa e Estados Unidos. Porém optou-se no presente estudo pela análise da mais recente legislação sobre tutela de dados adota na Europa, a "GDPR" que tem amplitude transacional com efetividade em toda a União Européia.

3.4 A *GENERAL DATA PROTECTION REGULATION* ("GDPR"): A NOVA PROTEÇÃO DE DADOS NA UNIÃO EUROPEIA

Até meados do andamento da pesquisa a experiência européia acerca de proteção de dados não se posicionava em uma uniforme lei comum para todos os estado membros da

[39]"Recentes instrumentos normativos, conforme verificado, apresentam referências cada vez mais explícitas a respeito de princípios de proteção de dados pessoais. A despeito de tais princípios ainda não estarem dispostos e ordenados em uma normativa geral e compreensiva de todas as diversas situações nas quais ocorre o tratamento de dados pessoais, é fato que respondem a uma demanda cada vez mais concreta e passível de verificação nas várias situações nas quais se tratam dados pessoais. A constatação de que tais princípios revelam, muito mais do que demandas setoriais, valores gerais e transversais a vários setores, bem como a sua estreita vinculação com a funcionalização de uma garantia fundamental de proteção aos dados pessoais que decorre da própria tutela da privacidadejustifica que tais princípios, mais do que serem considerados dentro do espectro de sua normatividade específica, sejam cada vez mais interpretados de forma extensiva para abarcar todas as situações nas quais possam proporcionar uma tutela da pessoa adequada às atuais necessidades na Sociedade de informação" (DONEDA, 2015, p.384) .

União Europeia. O artigo 8º da Carta de Direitos Fundamentais da União Europeia[40] positivou o direito fundamental à proteção de dados, influenciando todas as legislações posteriores na Europa, mas as mesmas ainda eram de competência nacional.

Na realidade o que se aplicavam em casos concretos eram as leis nacionais, a Diretiva 95/46/CE[41]e a Diretiva 2002/58/CE[42], que cuidavam da circulação e tratamento de dados pessoais nas comunicações eletrônicas e impunham aos Estados a obrigação de se adequarem futuramente aos seus parâmetros. Ocorre que este panorama mudou.

Após cinco intensos anos de deliberação, o texto final da "*General Data Protection Regulation*" ("GDPR"), foi aprovado em 27 de abril de 2016. Essa norma a partir de 25 de maio de 2018, ou seja, após o período de *vacaccio legis*, regerá a proteção de dados pessoais na União Europeia.

O impacto desta mudança é gigantesco[43]. Agora, ao contrário da Diretiva 95/46/CE que determinava a "internalização" ou "transposição" de valores apontados pela Diretiva em uma legislação nacional, e que, portanto, pode ser diferente de um país para o outro, a *General Data Protection Regulation* cria um regime jurídico único em todos os vinte e oito

---

[40]Artigo 8.º Proteção de dados pessoais
1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.
2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação.
3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente. Disponível em: <http://www.fd.uc.pt/CI/CEE/pm/Tratados/Nice/Carta%20Direitos%20Fundamentais.htm>. Acesso em: 13 de fevereiro de 2017.

[41] A Diretiva 95/46/CE define o tratamento de dados pessoais como uma operação ou conjunto de operações realizadas sobre dados pessoais, com ou sem meios automatizados, exemplificando a coleta, registro, organização, e similares, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição (art. 2º), e estipula em seu art. 7º alguns princípios aplicáveis a este tratamento como forma de assegurar a proteção dos dados pessoais envolvidos nestes processos. (GHISI; PEZZELA, 2015, p. 08)

[42] Destaca-se nesta Diretiva, o art. 5º versa sobre a confidencialidade dos dados nas comunicações eletrônicas, que não devem ser coletados e armazenados sem o consentimento das pessoas a que se referem, ressalvando-se ordens judiciais para tanto. Ainda, o art. 6º disciplina que os dados de tráfego, assim aqueles necessários para o estabelecimento de conexão e envio de comunicações, sejam desprezados tão logo o procedimento de comunicação se complete. (GHISI; PEZZELA, 2015, p. 09)

[43] Após cinco anos de intensas negociações, finalmente houve um acordo sobre o texto final da "General Data Protection Regulation" ("GDPR"), norma que possivelmente regerá a proteção à dados pessoais no velho continente, ainda pendente de aprovação no parlamento europeu. Um dos objetivos da modernização é não só proteger os dados pessoais dos cidadãos, mas também conferir segurança jurídica e permitir ao mercado usufruir ao máximo das oportunidades do intitulado "*Digital Single Market*". Como muito bem colocado por um dos principais interlocutores das discussões, Jan Philipp Albrecht, do Partido Verde Europeu, "irá remover barreiras e destravar oportunidades". Além dessa nova regulação, que substituirá a Diretiva 95/46/EC, de 1995 (época em que não era possível se quer vislumbrar o futuro digital atual), a reforma do panorama legal inclui uma nova diretiva para o setor de polícia e investigação criminal, que tem por objeto proteger os dados pessoais de vítimas, testemunhas e suspeitos mesmo em procedimentos investigatórios, em que a troca de informação pode ser essencial para a efetividade de eventual medida repressiva (MONTEIRO, texto *online*, 2016). Disponível em: <http://renatoleitemonteiro.com.br/analises-juridicas/a-nova-regulacao-de-protecao-de-dados-pessoais-aprovada-na-uniao-europeia-e-sua-influencia-no-brasil/>. Acesso em: 13 fev. 2017.

países membros da União Europeia, não exigindo qualquer tipo de habilitação legal por parte dos governos nacionais.

Por isso, mostra-se mais relevante observar e analisar os desdobramentos dessa nova norma que pode servir de orientação para as futuras discussões a nível nacional, do que se prender a análise de caso da Diretiva 95/46/CE que perderá sua validade. Evidentemente, por se tratar de uma legislação recente não existem ainda estudos aprofundados sobre o tema em nossa doutrina nacional.

Neste sentido, para um melhor aproveitamento no trabalho, optamos por uma análise seca da legislação, buscando extrair dela e de sua "exposição de motivos" os pontos pertinentes e relevantes da doutrina de proteção de dados para o Brasil.

O regulamento foi criado com o propósito[44] de criar regras específicas à proteção de dados pessoais de "pessoas singulares". Sua regulamentação busca proteger as garantias e direitos fundamentais em perfeita consonância com o reconhecimento elencado no artigo 8º da Carta de Direitos Fundamentais da União Europeia, que reconhece a proteção de dados como um direito fundamental em todo seu território.

Assim, a regulação cria um regime jurídico único em todos os 28 países membros, o que facilita os negócios e o controle por parte dos cidadãos uma vez que o sistema se tornou uniforme.

Além disso, seu escopo de atuação recai sobre todas as empresas e bancos de dados que processam informações pessoais na União Europeia ou para a União Europeia[45]. De tal sorte, se determinados serviços – como Facebook, Youtube e Google – tiverem interesse de se estabelecerem no território europeu e prestar serviços para cidadãos europeus, terão que se adequar em relação a eles sobre as mesmas regras. Com o respeito a seus direito

---

[44] *Article 1 Subject matter and objectives*
1. This Regulation lays down rules relating to the protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data.
2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
3. The free movement of personal data within the Union shall neither be restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.

[45] *Article 3 Territorial scope*
1. This Regulation applies to the processing of personal data in the context of the activities of na establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the European Union. 3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.

fundamentais e demais prerrogativas e princípios exigidos no regulamento. Aduz Rodotá (2015, p.01) sobre a amplitude do regulamento que:

> Deve projetar-se também sobre os novos "Senhores da Informação" que, por meio das gigantescas coletas de dados, governam as nossas vidas. Em face de tudo isso, a palavra "*privacy*" evoca não apenas uma necessidade de intimidade, mas sintetiza as liberdades que nos pertencem no mundo novo onde vivemos. O próprio modo de ser desses sujeitos – chamados Amazon ou Apple, Google ou Microsoft, Facebook ou Yahoo! – mostra-nos uma presença de oportunidade para a liberdade e a democracia e de um poder soberano exercido sem controle sobre a vida de todos.

A regulamentação apresenta em seu artigo 4º extenso rol de definições sobre o que seriam dados pessoais, os agentes intermediários públicos e privados que coletam, processam e armazenam esses dados bem como estabelecendo suas responsabilidades e limitando seus campos de atuação. Descreveu de forma clara e expressa essas definições, garantindo a segurança jurídica necessária no trato de uma tecnologia tão imprevisível como a computação.

Já no artigo 5º são apresentados os princípios que irão gerir a proteção de dados na União Europeia [46] nos quais se percebe que na legislação em tela utilizou-se do "núcleo comum" da principiologia da proteção de dados.

São eles: *lawfulness* (a utilização de dados deve ser de acordo com a lei; *fairness* (a utilização de dados deve ser de acordo com o que é justo); *transparency* (transparência ou publicidade); *purposelimitation* (propósitos limitados ou finalidade); *data minimisation* (dados limitados à utilização, ou seja, a proporcionalidade); *accuracy (*precisão ou qualidade); *storagelimitation* (limitação de armazenamento em caso de uso por órgãos públicos em caso

[46]*Article 5 :*
Principles relating to personal data processing
1. Personal data must be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency"); (b) collected for specified, explicit and legitimate purposes and not further processed in away incompatible with those purposes; further processing of personal data for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes shall, in accordance with Article 83(1), not be considered incompatible with the initial purposes; ("purpose limitation");
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation"); (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("accuracy"); (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data maybe stored for longer periods insofar as the data will be processed solely for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 83(1) subject to implementation of the appropriate technical and organizational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject ("storage limitation"); (eb) processed in a way that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ("integrity and confidentiality");
2. The controller shall be responsible for and be able to demonstrate compliance with paragraph 1 ("accountability").

de pesquisas ou interesse histórico) e *integrity and confidentiality* (integridade e confidencialidade atrelada à noção de segurança física e lógica).

A finalidade dos mesmos é a de assegurar um nível coerente de proteção das pessoas singulares em toda a União e da livre circulação de dados pessoais no mercado interno. A regulamentação não se pauta apenas em princípios, mas apresenta todas as regras de como deve ser feito, de modo a se legitimar estas práticas na esfera jurídica, funcionando além de um conteúdo programático ou principiológico.

Deste modo, ao abordar questões como retificação, tratamento ou atualização de informações nos dados pessoais, o regulamento não apenas prevê a possibilidade, mas determina de que é a competência para garantir estas praticas de maneira clara e objetiva.

Garantiu segurança jurídica e transparência aos operadores econômicos e de fornecer às pessoas "singulares" (com sentido parecido com a pessoa natural no Brasil) em todos os Estados-Membros da União Europeia o mesmo nível de direitos e obrigações e responsabilidades dos controladores e processadores no tratamento deseus dados pessoais.

Para tanto, o regulamento institui sanções equivalentes a serem aplicadas em caso de lesão ou abusividade em todos os Estados-Membros, bem como a estipulação de autoridades de supervisão com a participação de diferentes Estados-Membros sobre o cumprimento do mesmo por empresas que trabalhem com dados pessoais, no território europeu, ou fora se trataram de dados de europeus.

Reconhece que o bom funcionamento do mercado interno na União Europeia exige que a livre circulação de dados pessoais na União não seja restringida ou proibida por uma legislação de Proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais.

Compreendeu que a função da regulamentação não é a oposição ao uso da tecnologia ou a tentativa de um controle da mesma, mas a estipulação de regras para que se funcione em uma sociedade de informação capitalista e globalizada.

Destaca-se que o regulamento não se aplica ao tratamento de dados pessoais por uma pessoa singular nas suas atividades domésticas ou sociais, mas sim, em relação aos intermediários que fornecem os meios para processar dados pessoais para tais atividades pessoais ou domésticas. Por exemplo, não há aplicabilidade nas atividades realizadas pelas pessoas no Facebook, mas no que é feito com o registro dessas mesmas atividades.

Destaca-se também a abordagem do GDPR em relação ao consentimento informado e ao esquecimento, uma vez que são atentos às pessoas naturais em sua dignidade e na já trabalhada "autodeterminação informativa".

Neste sentido, cumpre apontar que o GDPR trabalha em seus artigos 7º[47] e 8º [48] o consentimento informado, uma vez que diversos estudos constataram que os usuários da rede não leem ou não compreendem os termos e as políticas de privacidade de um serviço ou aplicação. Cíntia Rosa Pereira de Lima (2014, p. 12) destaca a situação,

> Há vários estudos e pesquisas que demonstram os problemas que surgem pelo fato dos usuários não lerem as denominadas EULA. Estes motivos vão desde a pressa e ingenuidade do usuário à complexidade de compreensão dos termos usados pelo fornecedor. Robert A. Hillman elaborou um questionário e aplicou a 92 estudantes a fim de verificar se eles leem ou não os contratos de adesão eletrônicos. Apenas 4 alunos responderam que leem (4%); e quase metade, ou seja, 40 alunos (44%) responderam que não leem os contratos de adesão eletrônicos; 16 alunos responderam que leem a depender do termo (17%); 33 alunos leem dependendo do fornecedor (36%); e 34 alunos leem a depender do valor da transação eletrônica (37%). Destacando que os alunos podiam assinalar mais de um item parasua resposta.

O consentimento deve ser sempre anterior à manipulação dos dados, através de expressão clara do usuário que reconheça sua concordância não sódo tratamento de dados pessoais que lhe digam respeito, mas também do seu conhecimento da finalidade do uso destes. Se os dados serão utilizados para mais de uma finalidade, os termos devem ser claros sobre todos os usos.

Esta declaração pode ser escrita, por meio eletrônico ou até mesmo oral. Os termos desta manifestação de consentimento devem ser claros, tanto em relação ao aceite como da

---

[47] *Article 7:*
Conditions for consent
1. Where processing is based on consent, the controller shall be able to demonstrate that consent was given by the data subject to the processing of their personal data.
2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent must be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of the declaration which constitutes an infringement of this Regulation that the data subject has given consent to shall not be binding.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw consent as to give it.
4. When assessing whether consent is freely given, utmost account shall be taken of the fact whether, among others, the performance of a contract, including the provision of a service, is made conditional on the consent to the processing of data that is not necessary for the performance of this contract.

[48] *Article 8:*
Conditions applicable to child's consent in relation to information society services
1. Where Article 6 (1)(a) applies, in relation to the offering of information society services directly to a child, the processing of personal data of a child below the age of 16 years, or if provided for by Member State law a lower age which shall not be below 13 years, shall only be lawful if and to the extent that such consent is given or authorised by the holder of parental responsibility over the child.
1a. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.
2. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

finalidade, não podendo inferir-se que o silêncio ou a "pré-aceitação" (*box* dos termos com pré marcação em sites da internet) correspondam ao consentimento tácito.

Em relação ao esquecimento, nos artigos 16 e 17[49]abordam-se as retificações de dados por inexatidão de informações ou o "apagamento" em caso desses dados: quando não são mais necessários em relação às finalidades para as quais são recolhidos ou processados; quando o cidadão tenha retirado o seu consentimento; quando apresenta objeções para o tratamento de dados pessoais que lhe digam respeito; ou quando os tratamentos dos seus dados não cumpram o próprio regulamento. Traz ainda a possibilidade de remoção de dados de menores e crianças que não tem capacidade de discernir o uso e divulgação desses dados, inclusive quando já maior perceber este equívoco.

No entanto, a retenção dos dados pessoais é considerada legal onde é necessário, para o exercício do direito de liberdade de expressão e informação, para cumprimento de uma

[49]*Article 16:*
Right to rectification
The data subject shall have the right to obtain from the controller without undue delay the rectification of personal data concerning him or her which are inaccurate. Having regard to the purposes for which data were processed, the data subject shall have the right to obtain completion of incomplete personal data, including by means of providing a supplementary statemen
Article 17: Right to erasure ("right to be forgotten")
1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing of the data; (c) the data subject objects to the processing of personal data pursuant to Article 19(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing of personal data pursuant to Article 19(2); (d) they have been unlawfully processed; (e) the data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the data have been collected in relation to the offering of information society services referred to in Article 8(1).
2a. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the data, that the data subject has requested the erasure by such controllers of any links to, or copy or replication of that personal data.
3. Paragraphs 1 and 2 shall not apply to the extent that processing of the personal data is necessary: (a) for exercising the right of freedom of expression and information; (b) for compliance with a legal obligation which requires processing of personal data by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (c) for reasons of public interest in the area of public health in accordance with Article 9(2)(h) and (hb) as well as Article 9(4); (d) for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 83(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of the archiving purposes in the public interest, or the scientific and historical research purposes or the statistical purposes; (e) for the establishment, exercise or defence of legal claims.

obrigação legal ou para o desempenho de uma tarefa realizada no interesse público ou no exercício da autoridade pública.

Importa ressaltar que o texto final da GDPR foi proposto em 2012 e aprovado em 27 de abril de 2016, ou seja, sua tramitação praticamente pareou com o Marco Civil da Internet brasileiro (Lei n. 12.965/2014), promulgado em 23 de abril de 2014.

Tal convergência se justifica a partir da constatação de que os direitos da personalidade de maneira similar em todo o mundo conectado pela internet. Os sujeitos são projetados em representações digitais por redes sociais, perfis e cadastros pessoais em toda nova aplicação "personalizada" utilizada diuturna e massivamente pela população em busca de facilitação e comodidade, sem muito se ocupar com o preço a ser pago por isso.

Desta forma, são patentes as inspirações entre ambos, muito embora no caso do contexto brasileiro necessita-se de preencher muitas lacunas, justificando a necessidade uma legislação específica sobre a proteção de dados pessoais, como passaremos a demonstrar.

4. A PROTEÇÃO DE DADOS NO BRASIL

Apesar da existência abalizada na doutrina de princípios aplicáveis à proteção de dados e todo o amadurecimento jurídico sobre os mesmos, é sabido que inexiste no Brasil uma legislação específica. Nessa esteira, destaca Marcel Leonardi (2011, p. 02):

> O Brasil não tem normas específicas de proteção de dados pessoais. Nosso sistema jurídico tutela a privacidade de modo genérico, o que não é adequado para tratar das diversas hipóteses de tratamento de dados pessoais por empresas e governos.
> Nesse cenário de incerteza jurídica, todos perdem. Indivíduos não têm controle sobre o que acontece com seus dados. Empresas sérias descartam modelos de negócio inovadores, temendo ser confundidas com vigaristas que não respeitam consumidores. Autoridades públicas inescrupulosas aproveitam-se da lacuna legislativa para montar dossiês invasivos. O vácuo legislativo praticamente inviabiliza negócios envolvendo fluxo de dados entre o Brasil e os países que impõem padrões mínimos para a proteção de dados pessoais.

Não se nega os admiráveis e perceptíveis esforços legislativos recentes no país, mas corrobora-se o entendimento que ainda são muito difusos e incipientes, necessitando sempre de grande esforço hermenêutico para uma aplicabilidade concreta da proteção de dados no Brasil. Atualmente não há especificamente uma legislação brasileira sobre proteção de dados, mas uma percepção de alguns princípios de proteção de dados pessoais em outras normas.

Primeiramente, em matéria constitucional, a proteção da informação é resguardada ainda em uma dimensão negativa, na oposição entre as liberdades de expressão e de informação contra a proteção da personalidade e privacidade[50].

A proteção de dados não é expressa como um direito fundamental específico no Brasil, não encontrando essa normatização, sendo a escolha do ordenamento atrelar tal proteção na garantia de inviolabilidade da privacidade e intimidade e o sigilo nas

[50]Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação,independentemente de censura ou licença;
X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;
XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;
XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;
XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado.

comunicações de dados[51]·. Isso difere, neste sentido, do já apresentado artigo 8º da Carta de Direitos Fundamentais da União Europeia que expressamente positiva:"Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito".

A menção direta da Constituição Federal sobre proteção de dados se dá no inciso XII do já mencionado artigo 5º. Neste, determina-se a inviolabilidade do sigilo de comunicações, de dados e comunicações telefônicas, salvo por ordem judicial para fins de investigação criminal e instrução processual penal.

O direito à proteção de dados é revelado implicitamente no Brasil a partir da cognição dos riscos que o seu tratamento automatizado traz à proteção da personalidade e à luz das garantias constitucionais de igualdade substancial, liberdade e dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada (DONEDA, 2011, p. 13).

Buscando prevenir ofensas a esse direito, ainda sob um prisma de tutela, a Constituição estabeleceu o *habeas data*[52]para retificação e acesso a dados pessoais, embora nunca se tenha aplicado para dados digitais. Em tese, há guarida constitucional para a sua tutela por esse remédio constitucional, porém, somente quando o cidadão pleiteia essa garantia em juízo(DONEDA, 2011, p. 13).

Portanto, em esfera constitucional o que se tem é apenas uma tutela da proteção de dados atrelada à defesa da privacidade, buscando criar acessos ao cidadão de mecanismos eficazes e instrumentais de um primeiro controle de suas informações (acesso e retificação), limitando-se o alcance deste instituto[53].

Mas a proteção de dados, como foi visto durante o decorrer do estudo, não deve se pautar exclusivamente por instrumentos judiciais de tutela, mas na emancipação de quem

---

[51]Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

[52]Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
LXXII - 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;

[53]"Na verdade a questão formal que envolve o *habeas data* é uma questão de arquitetura constitucional e o acompanha desde sua gênese. O *habeas data* é um produto de seu tempo: tendo nascido como remédio para um problema específico, conforme mencionamos, que enfrenta o desafio de demonstrar sua aplicabilidade e eficácia em situações bastante diversas. Voltando ao momento da sua instituição, vemos que o constituinte brasileiro optou por não estabelecer um sistema de garantias individuais expressas positivamente, integrando o direito de acesso, retificação e outros com a principiologia relacionada á proteção de dados pessoais. Preferiu a técnica de reconhecer tais direitos através de uma ação voltada à sua defesa" (DONENDA, 2006, p.22).

detém os dados. Assim, "aquela que provavelmente é a maior limitação do *habeas data* não é perceptível pelo seu exame específico, porém deflui do contexto no qual se insere" (DONEDA, 2006, p. 337).

Esse entendimento foi seguido pelas normas infraconstitucionais que, de maneira específica, apresentam princípios de proteção de dados nas relações que tutelam.

Efetivamente, a primeira legislação a tratar do tema foi a Lei n. 8.078/1990, também conhecida como o Código de Defesa do Consumidor (CDC), que regula a manutenção e o cadastro de registro de consumidores em bancos de dados[54]. É perceptível alguns dos princípios do núcleo comum sobre proteção de dados, mas sem destacar os mesmos como pertencentes aum direito específico ou fundamental.

O CDC é uma lei de ordem pública e interesse social que foi elaborada por determinação constitucional[55]para regular a relação entre consumidores e fornecedores de produtos ou serviços. Quando o CDC exige que o consumidor seja informado previamente quando seu nome vai para algum cadastro ou banco de dados de proteção de crédito[56], está se garantindo o princípio da transparência. Mas, nesse caso, esse princípio está especificamente relacionado à transação comercial encampada e não necessariamente à tutela dos dados pelo cidadão.

---

[54]Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
§ 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
§ 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
§ 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.
§ 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.
§ 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.
§ 6º Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor.
Art. 44. Os órgãos públicos de defesa do consumidor manterão cadastros atualizados de reclamações fundamentadas contra fornecedores de produtos e serviços, devendo divulgá-lo pública e anualmente. A divulgação indicará se a reclamação foi atendida ou não pelo fornecedor.
§ 1° É facultado o acesso às informações lá constantes para orientação e consulta por qualquer interessado.
§ 2° Aplicam-se a este artigo, no que couber, as mesmas regras enunciadas no artigo anterior e as do parágrafo único do art. 22 deste código.

[55] Conforme expresso no art. 48 do Ato das Disposições Constitucionais Transitórias (ADCT): "O Congresso Nacional, dentro de cento e vinte dias da promulgação da Constituição, elaborará código de defesa do consumidor".

[56]Conforme a súmula 359 do STJ: Cabe ao órgão mantenedor do Cadastro de Proteção ao Crédito a notificação do devedor antes de proceder à inscrição.

Outros princípios patentes no CDCe com nuances mais próximas do almejado para uma proteção efetiva dos dados pessoais são os princípios da qualidade e do livre acesso, consoante Doneda (2015, p. 381):

> Os outros direitos do consumidor estabelecidos pelo CDC no que toca à proteção de seus dados pessoais são os direitos de acesso (correspondente ao princípio do livre acesso) e de retificação (correspondente ao princípio da qualidade), que possibilitam a ele consultar toda e qualquer informação pessoal a seu respeito armazenada "*em cadastros fichas, registros e dados pessoais e de consumo arquivados*" e, no caso de encontrar alguma incorreção, solicitar a retificação do dado (artigo 43, caput e § 3º). Na hipótese de lhe ser negado o exercício de tais direitos, o consumidor poderá se valer dos procedimentos judiciais ordinários (artigo 43,§ 4º) ou da já citada ação de *habeas data*.

Sobre o mesmo princípio da qualidade, alude Antônia Espíndola Longoni Klee e Guilher Magalhães Martins (2015, p.306):

> Logo, os fornecedores que conduzem negócios por meio eletrônico na internetdevem esclarecer como coletam e usam os dados dos consumidores em face do direito de informação por estes titularizados (artigo 6º, inciso III, do CDC), dando-lhes a oportunidade de corrigir possíveis imprecisões.
> Por ocasião do armazenamento destas informações, o consumidor, por força do artigo 43 do CDC, deverá ter acesso ao banco de dados da empresa que explora o site, sendo-lhe ainda permitido exigir sua correção, caso encontre alguma inexatidão, sob as penas do artigo 84 do CDC.

Desse modo, o CDC garante que os dados dos consumidores armazenados pelos prestadores de serviço em bancos de dados e cadastros sejam correspondentes à realidade, com possibilidades de retificação ou atualização.

Para completar essa"malha" de proteção da qualidade de dados ao consumidor, foi instituídaa Lei do Cadastro Positivo (Lei n. 12.414/2011), que regulamenta os bancos de dados e suas atividades com informação de adimplemento para formação de histórico de crédito.

Também esta legislação é igualmente responsável por trazer ao nosso ordenamento ineditamente mais princípios da proteção de dados pessoais como o princípio do livre acesso no seu artigo 5º [57], o princípio da necessidade[58], e o reforço do principio da finalidade no seu artigo 9º [59].

---

[57]Art. 5º São direitos do cadastrado:
II - acessar gratuitamente as informações sobre ele existentes no banco de dados, inclusive o seu histórico, cabendo ao gestor manter sistemas seguros, por telefone ou por meio eletrônico, de consulta para informar as informações de adimplemento;

Ademais, a referida lei protege os dados cadastrais tanto quanto o CDC ocupa-se exclusivamente das relações comerciais advindas da utilização dos dados pessoais do consumidor por empresas ou prestadores de serviço. Assim, apesar de toda inovação em estabelecer uma série de direitos e garantias da proteção de dados para o consumidor, inevitavelmente ela "já nasce com certos limites extrínsecos, o que se verifica não somente em relação à sua incidência - situações caracterizadas como relações de consumo – porém pelo caráter de suas disposições" (DONEDA, 2006, p.340).

Já a Lei do Acesso à Informação (Lei n. 12.527/2011) regulamenta o acesso a informações pessoais armazenadas por órgãos públicos, como previsto no inciso XXXIII[60] do artigo 5º, no inciso II[61] do § 3º do artigo 37 e no § 2º[62] do artigo 216da CF/1988.

Fundamentalmente é uma lei que garante o livre acesso aos dados pelo usuário. Seu artigo 31[63] afirma como será o tratamento das informações pessoais pela administração pública, mencionando-se a necessidade de transparência, de respeito à intimidade, à vida privada, à honra e à imagem das pessoas, bem como às liberdades e garantias individuais. Porém, novamente, a proteção é exclusiva aos dados armazenados em bancos de dados públicos.

III - solicitar impugnação de qualquer informação sobre ele erroneamente anotada em banco de dados e ter, em até 7 (sete) dias, sua correção ou cancelamento e comunicação aos bancos de dados com os quais ele compartilhou a informação;

[58]Art. 7º As informações disponibilizadas nos bancos de dados somente poderão ser utilizadas para:

I - realização de análise de risco de crédito do cadastrado; ou

II - subsidiar a concessão ou extensão de crédito e a realização de venda a prazo ou outras transações comerciais e empresariais que impliquem risco financeiro ao consulente.

Parágrafo único. Cabe ao gestor manter sistemas seguros, por telefone ou por meio eletrônico, de consulta para informar aos consulentes as informações de adimplemento do cadastrado.

[59]Art. 9º O compartilhamento de informação de adimplemento só é permitido se autorizado expressamente pelo cadastrado, por meio de assinatura em instrumento específico ou em cláusula apartada.

[60] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado.

[61] Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte:

§ 3º A lei disciplinará as formas de participação do usuário na administração pública direta e indireta, regulando especialmente:

II - o acesso dos usuários a registros administrativos e a informações sobre atos de governo, observado o disposto no art. 5º, X e XXXIII;

[62] Art. 216. Constituem patrimônio cultural brasileiro os bens de natureza material e imaterial, tomados individualmente ou em conjunto, portadores de referência à identidade, à ação, à memória dos diferentes grupos formadores da sociedade brasileira, nos quais se incluem:

§ 2º Cabem à administração pública, na forma da lei, a gestão da documentação governamental e as providências para franquear sua consulta a quantos dela necessitem.

[63]Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.

Demonstrando mais uma vezessa dispersão sobre a proteção de dados pessoais, a Lei "Carolina Dieckmann" (Lei n. 12.737/2012) dispõe sobre a tipificação criminal de delitos informáticos. Tal legislação incluiu o artigo 154-A no Código Penal, que trata da invasão de dispositivo informático alheio, conectado ou não à rede de computadores, através de violação indevida de mecanismos de segurança e com o objetivo de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou, ainda, instalar vulnerabilidades para obter vantagem ilícita[64]. Contudo, a lei aborda exclusivamente uma tutela contra invasões de privacidade ao se acessar criminosamente os dados pessoais.

Outro avanço significativo foi o reconhecimento do direito ao esquecimento, em virtude do crescente número de casos no Supremo Tribunal de Justiça envolvendo conflitos entre direito ao esquecimento e liberdade de expressão. Tal reconhecimento pela legislação ocorreu com a promulgação do enunciado nº 531 do Conselho Nacional de Justiça que literalmente informa que "a tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento".

Em meados do ano de 2106, entrou em vigor o Decreto presidencial n. 8.789/2016, que permite e disciplina o compartilhamento de base de dados entre órgãos e entidades federais, buscando o cruzamento de informações e o ganho de celeridade e eficácia na administração pública. Mas a possibilidade desse compartilhamento de dados não é a novidade, pois já ocorria por meio de convênios e acordos. O que o Decreto faz é dispensar a necessidade desses convênios e, assim, simplificar a transferência de dados, criando uma base legal única para toda comunicação de dados em todo nível federal.

---

[64] Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
I - Presidente da República, governadores e prefeitos;
II - Presidente do Supremo Tribunal Federal;
III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Apesar da argumentação oficial de que o Decreto visa à eficiência no manejar da coisa pública com maior economia e celeridade e que estes "cruzamentos" de dados já é comum, cumpre destacar que tais dados ainda são dados pessoais. Ainda que apenas no campo da especulação, a criação dessa *big data* é no mínimo problemática, uma vez que permite ao governo práticas como o *data mining* ou o *profiling* com os dados pessoais do cidadão sem o devido consentimento prévio do indivíduo. Aliás, o decreto nem reconhece esses dados como dados pessoais, denominando os mesmo como dados cadastrais.

Outra inovação foi o Decreto nº 8.777 de 2016 que instituiu a "Política de Dados Abertos" no âmbito do governo federal. A partir dela, todas as bases de dados de órgãos e entidades da administração pública federal serão disponibilizadas ao público em formato aberto, desde que não sejam sigilosos. Deste modo, facilita-se o controle externo sobre as atividades estatais sobre dados pessoais do cidadão, tendo a perfeita noção da extensão dos mesmos.

Conforme se percebe, a proteção de dados no Brasil se encontra de maneira dispersa e esparsa pelo ordenamento, o que dificulta doutrinariamente a sua aplicabilidade. Não por menos não é comum a utilização destes conceitos pelos tribunais. E, infelizmente, apesar de todos os avanços que serão abordados nessa dissertação,essa situação não se alterou com o Marco Civil da Internet (Lei n. 12.965/2014).

4.1 A PROTEÇÃO DE DADOS NO MARCO CIVIL DA INTERNET

Em 2014 foi promulgado o Marco Civil da Internet (Lei n. 12.965/2014), que apresenta e disciplina alguns aspectos de proteção de dados, talvez inspirados em discussões da GDPR, mas que também herda muito de uma visão do cidadão como consumidor, implementada a partir do CDC.

O Marco Civil estatuiu, em seu artigo 3º[65], princípios acerca do uso da internet como neutralidade, preservação da estabilidade, preservação da natureza participativa da rede,

[65]Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
II - proteção da privacidade;
III - proteção dos dados pessoais, na forma da lei;
IV - preservação e garantia da neutralidade de rede;
V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
VII - preservação da natureza participativa da rede;

liberdade no modelo de negócios e a proteção da privacidade e a proteção dos dados na forma da lei.

Além disso, apresentaram, em seu artigo 4º[66], os objetivos da disciplina do uso da internet no Brasil, e conceitos legais e técnicos para o uso da disciplina normativa[67], com um propósito mais abrangente: fundamentar a disciplina do uso da internet como um todo no Brasil. Neste sentido, esclarece Ronaldo Lemos (2015, p. 79) que:

> O Marco Civil é um projeto de lei singular. Não apenas por causa de seu conteúdo, mas também pelo processo que levou a sua criação, debate e aprovação. O Marco Civil estabelece princípios, direitos e deveres para a rede no Brasil de forma articulada com os princípios da democracia. Esse fato pode parecer trivial, mas não é. Vivemos hoje um momento em que a internet enfrenta grande fragmentação técnica e também jurídica.

Talvez um dos seus grandes méritos seja o fato de ser uma legislação que ainda em sua elaboração contou com a participação de entidades especializadas e pessoas físicas interessadas que puderam dar opiniões e sugestões. Ocorreram consultas públicas em sites oficiais[68] e debates online e presenciais o que colaborou para que o mesmo adquirisse rigor técnico e legitimidade entre o meio acadêmico.

VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

[66]Art. 4º A disciplina do uso da internet no Brasil tem por objetivo a promoção:
I - do direito de acesso à internet a todos;
II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;
III - da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e
IV - da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

[67]Art. 5º Para os efeitos desta Lei, considera-se:
I - internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;
II - terminal: o computador ou qualquer dispositivo que se conecte à internet;
III - endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;
IV - administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País;
V - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;
VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;
VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e
VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

[68]O site com o histórico destas contribuiçõesainda encontra-se disponível em: <http://www.culturadigital.br/marcocivil>. Acesso em: 13 de fevereiro de 2017.

Dessa forma, o Marco Civil da internet tem uma natureza principiológica e normativa. Principiológica por definir os princípios bases da rede no país e normativa por preencher as lacunas presentes em diversas leis brasileiras em relação a temas como o comércio e atutela da privacidade na internet, responsabilidade civil dos provedores e dos direitos e garantias fundamentais dos usuários na rede (LEMOS, 2015, p. 98).

Já em seu artigo 3º, incisos II e III, o Marco Civil já correlaciona a privacidade e a proteção de dados como princípios de utilização da internet no Brasil, muito embora apresente os mesmos como princípios distintos. Portanto, de maneira inédita, o Marco Civil reconhece o princípio da proteção de dados como um princípio exclusivo que não se delimita dentro do direito à privacidade[69].

Ainda, o parágrafo único do artigo 3º determina que os princípios expressos na lei não excluam ou invalidam outros previstos no ordenamento jurídico brasileiro ou nos tratados internacionais nos quais o Brasil seja parte. Desta forma, fica evidente que o Marco Civil regulamenta a internet para o uso por pessoas, em toda a sua dimensão humana de dignidade, e não o uso de simples consumidores.

Logo à internet brasileira devem se aplicar também princípios como da liberdade de expressão, igualdade e dignidade da pessoa humana (KLEE; MARTINS, 2015, p. 341).

Não por menos no artigo 6º[70] prevê-se que a utilização da internet levará em conta, além de sua natureza econômica, a promoção do desenvolvimento humano, econômico, social e cultural.

Destarte, apesar do Marco Civil da Internet não ser uma lei especifica sobre proteção de dados, é certo que em seu corpo normativo existem importantes avanços da sua doutrina. Assim:

> É bem verdade que o Marco Civil da Internet relega a uma lei específica posterior a efetivação da proteção aos dados pessoais (artigo 3º, inciso III) bem como às sanções por sua violação (artigo 11, § 4º). Nem por isso, entretanto, na ausência desta lei especial, haverá espaço para a manipulação indiscriminada de dados pessoais, uma vez que entre as garantias asseguradas às pessoas em suas operações via Internet está a vedação do fornecimento de dados a terceiros sem prévio consentimento livre e informado do titular dos dados (artigo 7º, inciso VII). No mesmo sentido, complementar à garantia anterior, está o direito de receber informações claras e completas sobre a coleta, uso, armazenamento de dados

[69] A inclusão em separado dos princípios de privacidade e proteção de dados, ainda que ligada histórica e funcionalmente à tutela da privacidade, dela é distinta por possuir escopo diverso. Esta abordagem remonta à solução adotada para tratar do tema pela Carta de Direitos Fundamentais da União Europeia, na qual ambos são mencionados em artigos distintos (artigos 7º e 8º) (DONEDA, 2015, p.382).

[70] Art. 6º Na interpretação desta Lei serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da internet, seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural.

> pessoais, com o adendo de que seu tratamento só poderá ocorrer se o princípio da finalidade justificar, se for lícito nos termos legais, ou estejam previstos em contratos (artigo 7º, inciso VII) (GHISI; PEZZELA, 2015, p.11).

Em seu artigo 7º[71], que trata dos direitos e garantias do usuário, estão presentes também princípios do núcleo comum. Nos incisos VII a IX, que dispõem sobre a coleta e o uso dos dados pessoais já se exigem a previsão do consentimento informado e expresso do titular ao assegurar ao usuário "o direito a informações claras e completas constates dos contratos de prestações de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações da internet", o que nada mais é do que a aplicação do princípio da finalidade.

E, ainda, no mesmo artigo 7º, inciso X, está previsto o direito à"exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvada as hipóteses de guarda obrigatória de registros prevista nesta Lei", que tipifica o direito ao esquecimento em termos similares ao GDPR europeu e ao enunciado nº 531 do CNJ.

---

[71]Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;
V - manutenção da qualidade contratada da conexão à internet;
VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
a) justifiquem sua coleta;
b) não sejam vedadas pela legislação; e
c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;
XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;
XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e
XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

No artigo 8º do Marco Civil[72], afirma-se que "a garantia do direito à privacidade e a liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet". Ainda, os artigos 10 a 12[73] abordam "*da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas*", preservando o sigilo pertinente à navegação na internet e os dados pessoais. Isso remete aos direitos fundamentais à privacidade, à intimidade e à liberdade expressos no texto constitucional, entendendo a importância da

[72]Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.
Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no caput, tais como aquelas que:
I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou
II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil.

[73]Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.
§ 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.
§ 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.
§ 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.
Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
§ 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
§ 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.
§ 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.
§ 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.
Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos artigos 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:
I - advertência, com indicação de prazo para adoção de medidas corretivas;
II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;
III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou
IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.
Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o caput sua filial, sucursal, escritório ou estabelecimento situado no País.

dimensão propagadora da personalidade humana que a internet possibilita, mas também em uma dimensão de garantia ou proteção negativa.

Por seu turno, nos artigos 13 a 15 está presente o princípio da segurança (ou segurança física e lógica), quando os mesmos tratam dos procedimentos exigíveis no ambiente de armazenamento de dados e da necessidade de adoção de medidas técnicas para a garantia de estabilidade de rede.

Ainda, o Marco Civil diz que cabe ao Estado garantir a privacidade e o sigilo dos dados pessoais e da navegação e possibilitar ao usuário, em caso de abusos, judicializar a questão em busca de ressarcimento (DONEDA, 2015, p. 383).

De toda sorte, embora o Marco Civil aborde e avance sobre questões de privacidade e proteção de dados, ainda possui diversas lacunas por se voltar em um enfoque generalista do uso da internet, desde sua dimensão de consumo até a qualidade da transmissão de dados, sem se estender claramente nas garantias de proteção de dados para o cidadão comum em toda e qualquer interação com a rede que tiver, seja esta com o poder público, empresarial ou entre particulares.

Talvez a lacuna mais alarmante seja o fato de que apesar de declarar o princípio da proteção dos dados pessoais, entendendo, portanto, a necessidade de sua guarida, o mesmo não define normativamente o que são "dados pessoais", além de outras contradições sobre a utilização e a guarda dos mesmos.

De maneira contundente, Rafael Zanata (2015, p. 453) elucida que:

> Com a lei n. 12.965/2014, alguns avanços são feitos no plano normativo para a proteção de dados pessoais. No entanto, tais avanços mostram-se limitados. Por exemplo, declara-se o princípio da proteção de dados pessoais(artigo 3º, inciso III), porém não há definição conceitual de "dados pessoais". Garante-se o registro de conexão, e de acesso a aplicações de internet (artigo 7º, inciso VII), porém garante-se a "exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação da internet" (artigo7º, inciso X), ressalvadas as hipóteses de guarda obrigatória de registros previstos na lei.

Essa ausência de definição se resolveu com a promulgação do Decreto n. 8.771/2016 que, em seu capítulo III, trata "da proteção aos registros, aos dados pessoais e às comunicações privadas". Assim como foi com o texto original do Marco, o decreto foi objeto de debates online em uma plataforma do Ministério da Justiça.

Tal decreto trouxe significativas e importantes mudanças na aplicação do Marco Civil da Internet. Determina, em seu artigo14[74], inciso I, que dado pessoal é o "dado

[74] Art. 14. Para os fins do disposto neste Decreto, considera-se:

relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa".

O Decreto também garante que a administração pública mediante determinação judicial, com finalidade fundamentada e previamente justificada, tenha acesso a registros de acesso e "dados cadastrais" de pessoas ou grupos específicos[75], mas seus órgãos competentes não poderão solicitar dados coletivos e genéricos. Da mesma forma, quando solicitarem, devem garantir mecanismos para que esses dados não sejam violados ou expostos, uma proteção velada aos chamados "dados sensíveis".

Ainda traz em seu art.13 [76]diretrizes de segurança e proteção física de dados, como a definição de responsabilidades das pessoas que terão acesso a dados armazenados, previsão

---

I - dado pessoal - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa; e

II - tratamento de dados pessoais - toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

[75]Art. 11. As autoridades administrativas a que se refere o art. 10, § 3º da Lei nº 12.965, de 2014, indicarão o fundamento legal de competência expressa para o acesso e a motivação para o pedido de acesso aos dados cadastrais.

§ 1º O provedor que não coletar dados cadastrais deverá informar tal fato à autoridade solicitante, ficando desobrigado de fornecer tais dados.

§ 2º São considerados dados cadastrais:

I - a filiação;

II - o endereço; e

III - a qualificação pessoal, entendida como nome, prenome, estado civil e profissão do usuário.

§ 3º Os pedidos de que trata o caput devem especificar os indivíduos cujos dados estão sendo requeridos e as informações desejadas, sendo vedados pedidos coletivos que sejam genéricos ou inespecíficos.

[76] Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança:

I - o estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários;

II - a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros;

III - a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014; e

IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.

§ 1º Cabe ao CGIbr promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais para o disposto nesse artigo, de acordo com as especificidades e o porte dos provedores de conexão e de aplicação.

§ 2º Tendo em vista o disposto nos incisos VII a X do caput do art. 7º da Lei nº 12.965, de 2014, os provedores de conexão e aplicações devem reter a menor quantidade possível de dados pessoais, comunicações privadas e registros de conexão e acesso a aplicações, os quais deverão ser excluídos:

I - tão logo atingida a finalidade de seu uso; ou

II - se encerrado o prazo determinado por obrigação legal.

de mecanismos de autenticação e identificação dos acessos aos registros com a criação de inventário do histórico de acesso a estes dados.

O decreto também exige em seu art. 12[77] a publicação de relatórios estatísticos que deverão conter o número de pedidos realizados por autoridades, à lista de provedores as quais os dados foram solicitados, o número de pedidos deferidos e indeferidos, e também o número de usuários afetados pelas solicitações.

Por fim, outra grande inovação do Decreto é a exigibilidade de que as empresas mantenham apenas "*a menor quantidade possível de dados pessoais, comunicações privadas e registros*", regra estampada no parágrafo 2º do artigo 13. Com isso, as empresas passam a ser obrigadas a excluir informações dos bancos de dados quando for atingida a finalidade que justificou sua coleta ou quando acabar o prazo de guarda determinado pela lei.

Certamente, o Decreto n. 8.771/2016 evolui o texto do Marco Civil, indo em direção a pontos que os projetos de lei de proteção de dados abordam. Mas apresenta a conceituação de dados pessoais, inclusive distinguindo os mesmos de dados cadastrais, de maneira muito genérica e pouco eficaz. O Decreto também se manteve omisso, como já verificado no Marco Civil, em exigir dos provedores a notificarem perdas e violação de dados aos consumidores e às autoridades.

Isto porque as lacunas e contradições apresentadas fundam-se no fato de que o Marco Civil da internet e seu decreto regulamentador, conforme já explicitamos, têm natureza principiológica, funcionando realmente como um "marco", mas ainda insuficiente para apresentar um corpo normativo robusto que garanta uma tutela eficiente da proteção de dados.

Dessa forma, ficam claramente ausentes definições e resoluções convincentes acerca de temáticas polêmicas e essenciais da proteção de dados, encontradas inclusive no GDPR europeu como: dados anonimizados, direito à portabilidade, autoridade de garantia, uso de dados pelo poder público, transferência internacional de dados, perfilamento, sanções por vazamentos dentre tantos outros.

Por não se tratar de uma legislação específica sobre proteção de dados, o Marco Civil não reconhece tal proteção como um direito fundamental atrelado ao exercício da privacidade e dos direitos da personalidade. Nem tampouco atina para sua natureza de autodeterminação

---

[77] Art. 12. A autoridade máxima de cada órgão da administração pública federal publicará anualmente em seu sítio na internet relatórios estatísticos de requisição de dados cadastrais, contendo:
I - o número de pedidos realizados;
II - a listagem dos provedores de conexão ou de acesso a aplicações aos quais os dados foram requeridos;
III - o número de pedidos deferidos e indeferidos pelos provedores de conexão e de acesso a aplicações; e
IV - o número de usuários afetados por tais solicitações.

informativa tão almejada nas sociedades de informação e adotada por praticamente todas as legislações modernas sobre o tema.

Para tanto, é urgente a aprovação de uma legislação específica e exclusiva sobre a proteção de dados, com conceituações claras e precisas sobre o que são os dados pessoais, qual o seu propósito e quais são possibilidades de utilização dentro de um regime normativo que respeite a dignidade humana.

4.2 O PROJETO DE LEI N. 5276/2016

Atualmente no Brasil, existem propostas legislativas concomitantes, em diferentes estágios e visões, sobre a proteção de dados. A presente dissertação optou pela análise do Projeto de Lei n. 5276/2016 (PL n. 5276/2016), de autoria do Ministério da Justiça, que se encontra perante o Senado brasileiro, sujeito à votação em regime de prioridade.

Porém reconhecem-se outras importantes iniciativas. Dentre elas, o projeto de lei nº 330 de 2013, que "*dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências*", que foi aglutinado a mais dois: o PL nº181 de 2014 que "*dispõe sobre o "fornecimento de dados de cidadãos ou empresas brasileiras a organismos estrangeiros*" e o PL nº 181 de 2014 que *"estabelece princípios, garantias, direitos e obrigações referentes à proteção de dados*".

A tramitação em conjunto – agora sob a denominação de PL nº 330 apenas - encontra-se ainda em trâmite nas comissões do Senado, estando sujeito, portanto, a diversas alterações no texto antes de ser encaminhada a votação pelo Congresso. Muito embora o projeto muito se equipare ao próprio PL nº 5276/16, não se adotará a análise do PL Nº 330 pelos seguintes motivos: há uma similitude entre os eixos básicos adotados entre ambos e o projeto está em um estágio muito inicial, distante ainda de um texto pronto para votação.

De toda sorte, se propôs à análise, ainda que breve, de alguns pontos específicos do projeto de lei nº 5276/16, pois seu texto está em conformidade com as mais avançadas legislações sobre o tema no mundo e o processo de sua elaboração em si representa uma inovação pela ampla participação popular e de setores interessados como o *InternetLab*, o *CGI,* o *ITS* , a *FGV* dentre tantos outros atores sociais que colaboraram.

As discussões sobre um anteprojeto de dados pessoais foram resultantes de uma parceria entre o Ministério da Justiça com o Observatório Brasileiro de Políticas Digitais da Fundação Getúlio Vargas do Rio de Janeiro. Toda a sua elaboração ocorreu a partir de panorama traçado por Danilo Doneda e Laura Schertel Mendes à frente do comitê de

formulação de políticas públicas para o Ministério da Justiça e com a participação efetiva do Comitê Gesto da Internet (CGI).

Dessa parceria surgiu o processo de construção de um anteprojeto de lei a ser enviado pelo Executivo ao Congresso Nacional. Para tanto, o governo federal, pelo Ministério da Justiça disponibilizou um endereço na internet para consulta pública, também no blog "Cultura Digital" e a partir de seminários anuais sobre proteção à privacidade de dados pessoais, que sempre conta com a presença e colaboração de acadêmicos, especialistas, profissionais e estudantes de diversas áreas de atuação (ZANATTA, 2015, p. 455).

Mobilizou-se a sociedade civil e empresas do ramo para contribuições, críticas e sugestões na elaboração deste pré-projeto apresentando as seguintes formas de participação pela plataforma digital[78]: com comentários sobre o texto da lei; com comentários por eixo temático e por envio de sugestões via arquivo "PDF". Deste modo, os participantes puderam interagir entre si, favorecendo o debate a própria divulgação do pré-projeto.

Essa digressão salienta que, desde o seu início, o PL n. 5276/2016 tem como marca maior a sua construção plural, democrática e horizontalizada, com a participação de diversos agentes que diuturnamente "constroem" a internet, desde os usuários até as empresas de aplicação e provedores de rede. O que coaduna com a doutrina da proteção de dados pessoais defendida por Rodotá.

Para o autor, em regra, a construção legislativa sobre a matéria é resultante de um processo de participação em larga escala de atores diversos, que se relacionam dispersivamente "em nível de formular projetos, confrontá-los, modificá-los, no intuito de sujeitá-los a um controle e a uma elaboração comuns, de mudar no setor da regulação jurídica formas e procedimentos típicos do método wiki" (RODOTÁ, 2015, p.03).

Para além deste mérito, o texto final levado à votação representaria um grande avanço sobre a proteção de dados pessoais, em relação ao que temos com o Marco Civil da Internet e regulamentações vigentes. Neste sentido:

> Embora a Lei n. 12.965/2014 contenha disposições sobre os temas da privacidade e de proteção de dados, considera-se que o tema seria mais bem resguardado com a

[78] Sobre todo o processo de construção do projeto, desde seus diálogos iniciais até a apresentação perante o congresso nacional, é extremamente pertinente uma leitura do relatório: *"O QUE ESTÁ EM JOGO NO DEBATE SOBRE DADOS PESSOAIS NO BRASIL? RELATÓRIO FINAL SOBRE O DEBATE PÚBLICO PROMOVIDO PELO MINISTÉRIO DA JUSTIÇA SOBRE O ANTEPROJETO DE LEI DE PROTEÇÃO DE DADOS PESSOAIS"*, doInternetLab disponível em:
<http://www.internetlab.org.br/wp-content/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf>. Acesso em: 13 de fevereiro de 2017.

> harmonização do Marco Civil da Internet e a Lei de Proteção de Dados Pessoais em elaboração no Poder Executivo. Uma lei específica sobre a proteção de dados pessoais é um passo imprescindível em direção a certa "civilização" no tratamento dos dados pessoais. Seria uma mensagem clara de que as empresas e os próprios governos têm que arcar com a responsabilidade de proteção de algo que é muito importante para o cidadão. (KLEE; MARTINS, 2015, p. 352)

O projeto apresenta-se em extensos treze eixos[79]: (i) escopo e aplicação da lei constantes nos artigos 1º ao 4º; (ii) a conceituação de dados pessoais, dados anônimos e dados sensíveis nos artigos 5º, 12 e 13; (iii) os princípios constantes no artigo 6º; (iv) sobre o consentimento nos artigos 7º e 11; (v) sobre o término do tratamento de dados nos artigo 14 e 15; (vi) sobre os direitos do titular nos artigos 16 aos 21; (vii) sobre a comunicação, interconexão e uso compartilhado de dados nos artigos 22 aos 27; (viii) sobre a transferência internacional de dados nos artigos 28 a 33; (xix) sobre a responsabilidade dos agentes nos artigos 34 a 41; (x) sobre a segurança e sigilo de dados pessoais nos artigos 42 ao 47; (xi) sobre as regras boas práticas nos artigos 48 e 49; (xii) sobre como assegurar direitos, garantias e deveres nos artigos 53 e 54 e (xiii) as disposições transitórias que discutem o termo de entrada em vigor da lei.

Porém, não se fará uma análise detalhada de todo o PL n. 5276/2016, pois o mesmo ainda será alvo de deliberação pelas casas legislativas e, portanto, poderá sofrer expressivas alterações durante o tramite. Na realidade, o propósito neste momento é apontar pontos relevantes que o projeto traz.

Já em seu artigo 1º, o Projeto de Lei sobre a proteção de dados pessoais (PL n. 5276/2016) reconhece que o tratamento de dados se dará em conformidade aos direitos e garantias fundamentais de liberdade e privacidade e em consonância com os direitos da personalidade[80]. Isso deixa claro que a proteção de dados pessoais é uma tutela da privacidade e de outros direitos da personalidade, conforme já apontado no estudo.

Também assegura ao usuário, em seu artigo 2º, o controle de seus dados pessoais[81], explicitando que a proteção de dados pessoais se fundará na autodeterminação informativa –

---

[79] Sobre os eixos apresentados, a divisão é a mesma proposta na consulta publica do anteprojeto. Disponível em: <http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/>. Acesso em: 13 fev. 2017.

[80] Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

[81] Art. 2º A disciplina da proteção de dados pessoais tem como fundamento o respeito à privacidade e:
I – a autodeterminação informativa;
II – a liberdade de expressão, de comunicação e de opinião;
III- a inviolabilidade da intimidade, da vida privada, da honra e da imagem;
IV- o desenvolvimento econômico e tecnológico;

que aparece expressa no texto- em conformidade com o núcleo comum da doutrina de proteção de dados. Ainda, no mesmo artigo, reconhece que a proteção de dados é um direito único, distinto da privacidade servindo como sua tutela.

No seu artigo 3º[82] determina que a lei tenha aplicabilidade a qualquer tratamento de dados realizados no território nacional ou de dados de indivíduos que aqui residem, aderindo ao mesmo entendimento do artigo 3º do GDPR. Excetua-se, conforme artigo 4º[83], os tratamentos de dados para fins exclusivamente pessoais ou para fins culturais, históricos e de segurança pública.

O PL n. 5276/2016 também inova no artigo 5º[84] ao corrigir a falha do Marco Civil da Internet, conceituando e oferecendo guarida a elementos necessários e pertinentes à proteção

---

V – a livre iniciativa, a livre concorrência e a defesa do consumidor.

[82] Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do países de sua sede ou serviços ou o tratamento de dados, desde que:

I – a operação de tratamento seja realizada no território nacional;

II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou tratamento de dados de indivíduos localizados no território nacional;

III – os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

Parágrafo único. Consideram-se coletados no território nacional os dados pessoais cujo titula nele se encontre no momento da coleta.

[83] Art. 4º Esta lei não se aplica ao tratamento de dados:

I – realizado por pessoa natural para fins exclusivamente pessoais;

II – realizado para fins exclusivamente jornalísticos, artísticos, literários ou acadêmicos;

III – realizado para fins exclusivos de segurança pública, de defesa nacional, de segurança do Estado ou de atividades de investigação e repressão de infrações penais.

[84] Art. 5º Para fins desta Lei, considera-se:

I – dado pessoal: dado relacionado à pessoa natural identificado ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa;

II – tratamento: toda operação realizada com dados pessoais, como asque se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

III – dados sensíveis: dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos.

IV- dados anonimizados : dados relativos a um titular que não possa ser identificado;

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

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

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

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

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

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

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

XII – anonimização; qualquer procedimento por meio do qual um dado pede a possibilidade de associação, direta ou indireta, a um indivíduo;

dos dados pessoais como: dados sensíveis[85], dados anonimizados, tratamento, banco de dados, titular, consentimento, dentre outros. Assim, a norma não se pauta apenas em princípios, mas instrumentaliza como a proteção deve ser feita, de modo a se legitimar estas práticas tecnológicas na esfera jurídica.

O artigo 6 [86] traz um compilado dos princípios da proteção de dados, rol apresentado no trabalho e defendido por Rodotá como comuns à grande maioria das legislações acerca de proteções de dado no mundo, inclusive a atual legislação europeia (GDPR). São literalmente apresentados os princípios: finalidade; adequação, necessidade; livre acesso; qualidade dos dados; transparência e segurança, além dos acrescidos prevenção e não discriminação.

O artigo 7º[87] traz os requisitos para o tratamento de dados pessoais. O requisito fundamental é o consentimento livre informado e expresso do titular, que poderá ser dado por

---

XIV- eliminação: exclusão definitiva de dado ou conjunto de dados armazenados em banco de dados, independente do procedimento empregado;
XV – uso compartilhado de dados: a comunicação, a difusão, a transferência internacional, a interconexão de dados pessoais ou o tratamento compartilhado de bancos de dados pessoais por órgão e entidades públicas, no cumprimento de suas competências legais, ou entre órgão e entidades públicos e entes privados, com autorização específica, para uma ou mais modalidades de tratamento delegados por esses entes públicos.

[85] Diante da gravitação de informações e dados, o interesse pela proteção de dados pessoais recebe influxo especial, inclusive com o reconhecimento de caráter jurídico, ante a inserção nas categorias de direitos humanos e direitos fundamentais. Importante registrar que dados pessoais consistem em conjunto de informações que permitem a identificação de pessoas no momento ou posteriormente, e desdobram-se ainda na categoria dos dados sensíveis quando atinem à ideologia, religião, crença, raça, saúde (GHISI; PEZZELA, 2015, p. 04).

[86] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - finalidade: pelo qual o tratamento deve ser realizado para finalidades legítimas, específicas, explícitas e informadas ao titular, não podendo ser tratados posteriormente de forma incompatível com essas finalidades:
II - adequação: pelo qual o tratamento deve ser compatível com as suas finalidades e com as legítimas expectativas do titular, de acordo com o contexto do tratamento;
III - necessidade: pelo qual o tratamento deve se limitar ao mínimo necessário para a realização das suas finalidades, abrangendo dados pertinentes, proporcionais e não excessivos emrelação às finalidades do tratamento de dados;
IV - livre acesso: pelo qual deve ser garantida aos titulares consulta facilitada e gratuita sobre as modalidades de tratamento e sobre a integralidade dos seus dados pessoais;
V - qualidade dos dados: pelo qual devem ser garantidas aos titulares a exatidão, a clareza, relevância e a atualização dos dados, de acordo com a periodicidade necessária para o cumprimento da finalidade de seu tratamento;
VI - transparência: pelo qual devem ser garantidas aos titulares informações claras, adequadas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento;
VII - segurança: pelo qual devem ser utilizadas medidas técnicas e administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e aptas a proteger dos pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão:
VIII - prevenção: pelo qual devem ser adotadas medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX - não discriminação: pelo qual o tratamento não pode ser realizado para fins discriminatórios.

[87] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
I- mediante o fornecimento pelo titular de consentimento livre, informado e inequívoco;
II – para o cumprimento de uma obrigação legal pelo responsável;
III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis ou regulamentos;
IV - para a realização de pesquisa histórica, científica ou estatística, garantida., sempre que possível, a anonimização dos dados pessoais;

escrito ou por outro meio que o certifique, com possibilidade de sua revogação e a obrigatoriedade das informações pertinentes e necessárias para o mesmo.

Finalmente, em seus artigos 53 e 54, o projeto de lei propõe a criação de um órgão fiscalizador específico, competente para: zelar pela proteção de dados pessoais; elaborar diretrizes de uma política nacional sobre o tema; realizar auditorias nos envolvidos em práticas de manipulação de dados; a divulgação e o estimulo de boas práticas na utilização dos dados pessoais entre outras atribuições

Esse órgão – denominado de Conselho Nacional de Proteção de Dados Pessoais e da Privacidade- contaria com representantes dos três poderes juntamente com membros da sociedade civil, da academia, do setor privado e do CGI.

Como se percebe muitas das inovações apontadas se apresenta em termos semelhantes à "*General Data Protection Regulation*" aprovado e de atual aplicabilidade na Europa, buscando um caráter de tutela pelo Estado dos dados pessoais. Tal tutela é necessária, uma vez que o Brasil, como foi demonstrado, já se encontra inserido na sociedade de informação

Neste sentido, Doneda (2015, p. 384) afirma que:

> Recentes instrumentos normativos, conforme verificado, apresentam referências cada vez mais explícitas a respeito de princípios de proteção de dados pessoais. A despeito de tais princípios ainda não estarem dispostos e ordenados em uma normativa geral e compreensiva de todas as diversas situações nas quais ocorre o tratamento de dados pessoais, é fato que respondem a uma demanda cada vez mais concreta e passível de verificação nas várias situações nas quais se tratam dados pessoais. A constatação de que tais princípios revelam, muito mais do que demandas setoriais, valores gerais e transversais a vários setores, bem como a sua estreita vinculação com a funcionalização de uma garantia fundamental de proteção aos dados pessoais que decorre da própria tutela da privacidade justifica que tais princípios, mais do que serem considerados dentro do espectro de sua normatividade específica, sejam cada vez mais interpretados de forma extensiva para abarcar todas as situações nas quais possam proporcionar uma tutela da pessoa adequada às atuais necessidades na "sociedade de informação" .

De fato, nas sociedades de informação, como é a sociedade brasileira atual, nos dizeres de Maria Celina Bodin de Moraes (2010, p. 14), "nós somos as nossas informações,

---

V - quando necessário para a execução de um contrato ou de procedimentos preliminares relacionados a um contrato do qual é parte o titular, a pedido do titular dos dados;
VI - para o exercício regular de direitos em processo judicial ou administrativo;
VII - para a proteção da vida ou da incolumidade fisica do titular ou de terceiro;
VIII - para a tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
IX - quando necessário para atender aos interesses legítimos do responsável ou de terceiro, exceto no caso de prevalecerem interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for menor de idade.

pois elas nos definem nos classificam, nos etiquetam; portanto, a privacidade hoje se manifesta essencialmente em ter como controlar a circulação".

No entanto, assim como a "*General Data Protection Regulation*", o projeto trata de uma concepção qualitativamente diferente de tutela da privacidade. Muito além de oferecer uma doutrina completa para a proteção dos dados pessoais, objetiva construir um novo entendimento. Protege-se o "direito à autodeterminação informativa", que ainda não encontrou guarida adequada no ordenamento jurídico, além de confirmar a distinção existente entre proteção de dados e privacidade.

Destarte, a aprovação de uma lei específica sobre a proteção de dados pessoais nestes moldes, representaria um avanço imprescindível em direção à construção de uma nova civilidade na sociedade de informação brasileira. Representaria a vitória de uma nova visão sobre o trato de dados pessoais e da privacidade, uma vez que determina que as empresas, os indivíduos e o próprios governo possuem a responsabilidade conjunta na tutela dos dados.

Deste modo, apesar dos avanços do texto proposto, a tutela da proteção de dados não se efetivará apenas com a sua promulgação. É necessário que a sociedade em suas práticas efetive a matéria, dando lhe aderência e solidez.

CONCLUSÃO

Conforme explanado durante toda a dissertação, o avanço evidente das tecnologias de informação e comunicação na sociedade impõe ao Direito imensos desafios, não sendo mais possível pensar na privacidade nos moldes tradicionais.

Atualmente, privacidade é vinculada à dimensão intersubjetiva no constante fluxo de dados pessoais da internet. Desse modo, interações sociais e atividades – que antes se davam no seio de seu lar, cercado pela intimidade da família ou de sua privacidade individual –se realizam por meio da tecnologia.

Basta pensar que toda atividade desempenhada em um computador pode ser monitorada, formando um "perfil" do usuário,utilizado com extrema eficiência por empresas que buscam um público alvo para seus produtos, ou para auxiliar a prestações de serviços públicos. Com esta simples ilação, percebe-se que a tutela dessas informações é um novo e importante elemento a ser pensado por qualquer regime democrático que pretenda defender a privacidade e a intimidade de seus cidadãos.

Assim, o direito à privacidade não pode ser mais abordado apenas com uma visão individualista e subjetiva, como um "direito a ser deixado só", que recebe do Estado uma tutela negativa que impede o seu vilipêndio. Nesse entendimento, a doutrina vem cada vez mais atrelando a privacidade ao controle pelo cidadão de suas informações e dados pessoais nos meios automatizados de informação, como internet e bancos de dados.

Na realidade, a privacidade se apresenta com uma faceta de autodeterminação informativa do indivíduo na sociedade de informação. Nela, a existência humana e o exercício dos direitos da personalidade passaram a ter uma dimensão informacional. Portanto, os indivíduos são representados por informações pessoais que recebem tratamentos pela tecnologia e livremente circulam pela internet.

Isto graças ao amadurecimento tecnológico, que aumentou vertiginosamente a capacidade de se coletar, processar e armazenar informação a tal ponto que todo registro de atividade do indivíduo por meio eletrônicos pode se converter em dados que são altamente valorizados pelo setor produtivo e instituições públicas, sendo, inclusive, reconhecidos como recurso de base.

Desse modo, a defesa da privacidade não pode ser mais sustentada por um sistema jurídico que meramente controle ou limite o uso de computadores e *smartphones*, mas a partir da reflexão sobre o impacto que o uso cotidiano dessas tecnologias causa na sociedade.

Nesse sentido, deve-se proteger a circulação livremente disponibilizada e ofertada pelos indivíduos de um uso abusivo por empresas e governos. Ainda, deve-se garantir o menor limite possível de manuseamento das informações pessoais sem a anuência ou o conhecimento dos indivíduos, projetando-os ao controle de seus dados.

A privacidade deve ser garantida a partir da problematização de situações específicas, nas quais se tenciona o livre exercício de direitos intersubjetivos dos indivíduos com as demandas dos agentes que manipulam essas tecnologias. Essa garantia passa da compreensão dos poderes políticos e econômicos que surgiram no tratamento das informações como recurso base.

Para tanto, é necessário conceituar e distinguir as informações pessoais dos dados pessoais, que se apresentam como informações tratadas ou com a possibilidade de serem tratadas pela tecnologia. A individualização conceitual dos dados garante uma tutela de maior abrangência da privacidade, pois projeta a proteção muito além da dimensão negativa de se impedir abusos, com a promoção do próprio indivíduo como responsável principal sobre os usos dos mesmos.

Por conseguinte, quando se compreende os dados como um campo conceitual que engloba desde a "pré-informação" até a informação já tratada pela tecnologia, a tutela dos mesmos garante que a circulação de informações pessoais ocorra durante todo seu processo sob o controle do indivíduo. Logo, a proteção de dados pessoais funciona efetivamente como um "garantidor" da personalidade humana e da autodeterminação informativa que é a dimensão intersubjetiva da privacidade.

Para uma efetiva proteção da privacidade, contemporaneamente não é mais eficaz enxergar a proteção de dados como uma dimensão subalterna daquela. Não por menos, as legislações mais pertinentes sobre o tema, como a recém aprovada *General Data Protection Regulation*, que regulamenta a proteção de dados pessoais na União Europeia, já tratam o direito à proteção de dados como um direito fundamental, merecedor de legislação específica e guarida constitucional própria.

Nestas regulamentações, o direito à proteção de dados é um direito "garantidor" do exercício da privacidade que se ancora na autotutela informativa do indivíduo e em outros mecanismos que garantem o exercício dos direitos da personalidade nos meios eletrônicos e virtuais.

Para que isso ocorra, as regulamentações elevam o padrão coletivo de proteção, fortalecendo o direito das pessoas em relação às entidades e empresas que coletam seus dados a partir de um arcabouço principiológico específico e claro.

A proteção de dados pessoais ultrapassa uma visão patrimonialista, para a proteção da própria personalidade humana. Assim, as salvaguardas legais não devem ser baseadas em reconhecer os indivíduos como donos dos dados a seu respeito.

Na realidade a proteção de dados pessoais envolve o controle dos mesmos pelas pessoas na autodeterminação informativa, mas também na tutela do Estado dos dados sensíveis, anonimizados e da própria segurança e regularidade do processo de tratamento destes dados.

Assim, conforme se constatou no presente estudo, apesar das demandas claras e evidentes de uma sociedade de informação vívida e expressiva, no Brasil ainda não possuímos uma legislação específica sobre proteção de dados, estando defasado perante o resto do mundo.

O atual panorama legal brasileiro acerca da matéria não possui guarida expressa da proteção de dados como um direito fundamental distinto, sendo na realidade protegida por tutelas estatais contra o abuso à manipulação das informações pessoais.

Conta com legislações como o Código de Defesa do Consumidor (CDC), a Lei "Carolina Dieckmann", e a Lei do Cadastro Positivo, que tratam de casos específicos e de pouco amplitude para uma real proteção de dados, não construindo um regime jurídico efetivo para o exercício da autodeterminação informativa.

Por outro lado, o Marco Civil da Internet ocupou-se de regulamentar a internet como um todo, desde sua prestação de serviços até a qualidade dos dados que transitam na rede. Em relação à proteção de dados, todavia, funciona muito mais como uma norma principiológica, que reconhece a necessidade da tutela, mas não apresenta os conceitos e mecanismos necessários para a mesma.

Embora apresente muitos avanços – como o reconhecimento da proteção de dados como um direito, a necessidade do consentimento livre e informado, o direito ao esquecimento e tantos outros mecanismos de proteção de dados pessoais – o Marco Civil da Internet se pautou pela guarida judicial como forma de controle pelo cidadão.

Com o Decreto nº 8.771, de 11 de Maio de 2016, finalmente se apresentou a conceituação de dados pessoais, inclusive distinguindo os mesmos de dados cadastrais, mas de maneira muito genérica e pouco eficaz.

E, ainda, se abordou a proteção desses dados como uma tutela negativa, impedindo o abuso indevido, mas não apresentando qualquer disciplina para o seu uso correto e produtivo, como se exige na sociedade de informação.

O nosso bojo institucional atual, ainda que amplo o suficiente para novas interpretações hermenêuticas acerca do alcance da privacidade e da proteção dos dados pessoais, seguramente não possui uma legislação adequada para enfrentar as novas realidades apresentadas pela sociedade da informação que surgiram dos últimos avanços tecnológicos.

Conclui-se, pois, que fica explicita a necessidade de um marco regulatório específico sobre proteção de dados, uma vez que a indefinição e dispersão legislativas criam incertezas sobre o manuseio de informações pessoais do cidadão, impossibilitando uma efetiva tutela dos dados pessoais pela sociedade.

REFERÊNCIAS

ASSOCIAÇÃO INTERNETLAB DE PESQUISA EM DIREITO E TECNOLOGIA. O que está em jogo no debate sobre dados pessoais no Brasil? Relatório final sobre o debate público promovido pelo Ministério da Justiça sobre o Anteprojeto de lei de proteção de dados pessoais (2016). Disponível em: <http://www.internetlab.org.br/wpcontent/uploads/2016/05/reporta_apl_dados_pessoais_final.pdf>. Acesso em: 13 fev. 2017.

BAIÃO, Kelly Sampaio; GONÇALVES, Kalline Carvalho. A garantia da privacidade na sociedade tecnológica: um imperativo à concretização do princípio da dignidade da pessoa humana.*Civilistica.com*.Rio de Janeiro, a. 3, n. 2, jul.-dez./2014. Disponível em: <http://civilistica.com/a-garantia-da-privacidade-na-sociedade-tecnologica-um-imperativo-a-concretizacao-do-principio-da-dignidade-da-pessoa-humana/>. Acesso em: 13 de fevereiro de 2017.

BARROS, Alice Monteiro de. *Curso de Direito do Trabalho*. 7. ed. São Paulo: Ltr, 2011.

BELMONTE, Alexandre Agra. Responsabilidade por danos morais nas relações de trabalho. *Revista TST*, Brasília, v. 73, n. 2, p. 158-185, abr./jun. 2007

BOBBIO, Norberto. *A Era dos Direitos*. Trad. Carlos Nelson Coutinho. 6. reimp. Rio de Janeiro: Elsevier,2004.

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil:* promulgada em 5 de outubro de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/ConstituicaoCompilado.htm>. Acesso em: 13 fev. 2017.

_____. *Lei n. 8.078, de 11 de setembro de 1990*. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8078.htm>. Acesso em: 13 fev. 2017.

_____. *Lei n. 12.414, de 09 de junho de 2011*. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>. Acesso em: 13 fev. 2017.

_____. *Lei n. 12.527, de 18 de novembro de 2011*. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 13 fev. 2017.

_____. *Lei n. 12.737, de 30 de novembro de 2012*. Dispõe sobre a tipificação criminal dos delitos informáticos; altera o Decreto-Lei n. 2.848, de 07 de dezembro de 1940 – Código Penal; e dá outras previdências. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 13 fev. 2017.

_____. *Lei n. 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 13 fev. 2017.

_____. *Decreto n. 8. 771, de 11 de maio de 2016.* Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm>. Acesso em: 13 fev. 2017.

_____. *Projeto de Lei n. 5276/2016*. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378>. Acesso em: 13 fev. 2017.

BOBBIO, Norberto. *A Era dos Direitos*. Trad. Carlos Nelson Coutinho. 6ª. reimp. Rio de Janeiro: Elsevier, 2004.

BUCAR, Daniel. Controle temporal de dados: o direito ao esquecimento. *Civilistica.com.*, Rio de Janeiro, a. 2, n. 3, p. 01-17, jul.-set./2013. Disponível em:<http://civilistica.com/wp-content/uploads/2015/02/Bucar-civilistica.com-a. 2.n.3.2013.pdf>. Acesso em: 13 fev. 2017.

CANOTILHO, Joaquim José Gomes. *Direito constitucional e teoria da constituição*. 7. ed. Lisboa: Almedina, 2003.

CASTELLS, Manuel. *A sociedade em rede*. A era da informação: economia, sociedade e cultura. Trad. Roneide Venâncio Majer. 7. ed. São Paulo: Paz e Terra, 2003.

COELHO, Fábio Ulhoa. O Direito à Privacidade no Marco Civil da Internet. In: LUCCA, Newton de; FILHO, Adalberto Simão; LIMA, Cíntia Rosa Perereira de (Coords.). *Direito & Internet III – Tomo I: Marco Civil da internet (Lei n. 12956/2014)*. São Paulo: Quartier Latin, 2015.p.503-516.

CORTE EUROPEIA DOS DIREITOS HUMANOS. *Convenção para a Proteção dos Direitos do Homem***.** Estrasburgo-França: Conselho da Europa, [s. d.].Disponível em: <http://www.echr.coe.int/Documents/Convention_POR.pdf>.Acesso em: 13 de fevereiro de 2017.

CUNHA JÚNIOR, Dirleyda.*Curso de Direito Constitucional.* 3. ed., rev., ampl. e atual. Salvador: JusPodivm,2009.

DALBERIO, Osvaldo; DALBERIO, Maria Célia Borges. *Metodologia Científica: desafios e caminhos.* 2. ed. São Paulo: Paulus, 2011.

DONEDA, Danilo Cesar Maganhoto. A proteção de dados pessoais como um direito fundamental. Revista *Espaço Jurídico Journal of Law*, Joaçaba-SC, v. 12, n. 02, p. 91-108, jul./dez. 2011.

_____. Considerações iniciais sobre bancos de dados informatizados e o direito à privacidade. In: TEPEDINO, Gustavo (Org.). *Problemas de direito civil-constitucional*. Rio de Janeiro: Renovar, 2000.p. 111-136.

_____. *Da Privacidade à Proteção de Dados Pessoais*. São Paulo: Renovar, 2006.

_____. Princípios de Proteção de Dados Pessoais. In: LUCCA, Newton de; FILHO, Adalberto Simão; LIMA, Cíntia Rosa Perereira de (coords.). *Direito & Internet III – Tomo I: Marco Civil da internet (Lei n. 12956/2014)*. São Paulo: Quartier Latin, 2015.p.369 – 384.

_____. Iguais mas separados: o habeas data no ordenamento brasileiro e a proteção de dados pessoais. *Cadernos da Escola de Direito e Relações Internacionais*, Curitiba, n. 09, p. 14-33, 2008.

_____. Privacidade, vida privada e intimidade no ordenamento jurídico brasileiro. Da emergência de uma revisão conceitual e da tutela de dados pessoais. *Revista Âmbito Jurídico*, RioGrande-RS, XI, n. 51, mar. 2008. Disponível em: <http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=2460>. Acesso em: 13 fev. 2017.

_____. Reflexões sobre proteção de dados pessoais em redes sociais. *Revista Internacional de Protección de Datos Personales*, Bogotá, n. 01, p. 02-13, jul.- dic./2012.
DINIZ, Maria Helena. *Curso de direito civil brasileiro*: teoria geral do direito civil. 25. ed. São Paulo: Saraiva, v. 1, 2008.

EBERLE, Simone. *A capacidade entre o fato e o Direito*. Porto Alegre: Sergio Antonio Fabris Editor,2006.

EUROPEAN COMMISSION. Justice *Protection of personal data*. Disponível em: <http://ec.europa.eu/justice/data-protection/index_en.htm>. Acesso em: 13 fev. 2017.

FÁBIO, André Cabette. O que é 'pós-verdade', a palavra do ano segundo a Universidade de Oxford. *Nexo Jornal*, nov. 2016. Disponível em: <https://www.nexojornal.com.br/expresso/2016/11/16/O-que-%C3%A9%E2%80%98p%C3%B3s-verdade%E2%80%99-a-palavra-do-ano-segundo-a-Universidade-de-Oxford>. Acesso em: 13 fev. 2017.

FACHIN, Zulmar. *Curso de Direito Constitucional*. 5. ed. Rio de Janeiro: Forense, 2012.

FARIAS,Edilsom Pereira. *Colisão de direitos*: a honra, a intimidade, a vida privada e a imagem versus a liberdade de expressão e informação. 2. ed. Porto Alegre: Sergio Antonio Fabris Editor,2000.

FGV-CTS, *Relatório de Políticas de Internet: Brasil 2011*. São Paulo: Comitê Gestor da Internet no Brasil, 2012.

FURASTÉ, Pedro Augusto. *Normas técnicas para o trabalho científico***:** explicitação das normas da ABNT. 17. ed. Porto Alegre: Dáctilo Plus,2013.

GHISI, Silvano. PEZZELA, Maria Christina Cereser. A manipulação de dados pessoais nas relações de consumo e o sistema "crediscore". *Civilistica.com*. Rio de Janeiro, a. 4, n. 1, jan.-jun./2015. Disponível em: <http://civilistica.com/wp-content/uploads/2015/08/Pezzella-e-Ghisi-civilistica.com-a.4.n.1.2015.pdf >. Acesso em:13 fev. 2017.

GIANNOTTI, Edoardo. *A tutela constitucional da intimidade.* Rio de Janeiro: Forense, 1987.

GONÇALVES, Carlos Roberto. *Direito civil brasileiro: responsabilidade civil*. 3. ed. São Paulo: Saraiva, 2008. KANT, Immanuel. Fundamentação da Metafísica dos Costumes. Trad. Paulo Quintela. Lisboa: Edições 70, 2007.

JUNIOR, Irineu Francisco Barreto. Proteção da Privacidade e de Dados Pessoais na Internet: O Marco Civil da rede examinado com fundamentos nas teorias de Zygmunt Bauman e Manuel Castells. In: LUCCA, Newton de; FILHO, Adalberto Simão; LIMA, Cíntia Rosa Perereira de (Coord.). *Direito & Internet III – Tomo I: Marco Civil da internet (Lei n. 12956/2014)*. São Paulo: Quartier Latin, 2015.p. 405 -430.

KANT, Immanuel. *Fundamentação da Metafísica dos Costumes.* Trad. Paulo Quintela. Lisboa: Edições 70, 2007.

KLEE, Antonia Espíndola Longoni; MARTINS, Guilherme Magalhães, A Privacidade, a Proteção dos Dados e dos Registros Pessoais e a Liberdade de Expressão: Algumas Reflexões sobre o Marco Civil da Internet no Brasil (Lei nº 12.965/2014). In: LUCCA, Newton de; FILHO, Adalberto Simão; LIMA, Cíntia Rosa Pereira de (Coord.). *Direito & Internet III – Tomo I: Marco Civil da internet (Lei n. 12956/2014)*. São Paulo: Quartier Latin, 2015.p. 291 - 368.

LEMOS, Ronaldo. Uma Breve História da Criação do Marco Civil. In: LUCCA, Newton de FILHO, Adalberto Simão; LIMA, Cíntia Rosa Pereira de (Coord.). *Direito & Internet III – Tomo I: Marco Civil da internet (Lei n. 12956/2014)*. São Paulo: Quartier Latin, 2015.p.79 - 101.

LEONARDI, Marcel. Marco Civil da Internet e Proteção de Dados Pessoais. In: LUCCA, Newton de; FILHO, Adalberto Simão; LIMA, Cíntia Rosa Pereira de (Coord.). *Direito & Internet III – Tomo I: Marco Civil da internet (Lei n. 12956/2014)*. São Paulo: QuartierLatin, 2015.p. 517-538.

LIMA, C. C. C.; MONTEIRO, R. L. Panorama brasileiro sobre a proteção de dados pessoais: discussão e análise comparada. *A to Z: novas práticas em informação e conhecimento*, Curitiba, v. 2, n. 1, p. 60-76, jan./jun. 2013. Disponível em: <http://www.atoz.ufpr.br>. Acesso em: 13 fev. 2017.

LIMA, Cíntia Rosa Pereira de. *O ônus de ler o contrato no contexto da "ditadura" dos contratos de adesão eletrônicos*. In: ROVER, Aires José; CELLA, José Renato Gaziero;

Ayuda, Fernando Galindo (Coord.). Direito e novas tecnologias I. Florianópolis: CONPEDI, 2014.

_____; BIONI, Bruno Ricardo. A Proteção dos Dados Pessoais na Fase de Coleta: Apontamentos sobre a Adjetivação do Consentimento Implementada pelo Artigo 7, Incisos VIII e IX, do Marco Civil da Internet a partir *da Human Computer Interaction e da Privacy by Default*.In: LUCCA, Newton de; FILHO, Adalberto Simão; LIMA, Cíntia Rosa Pereira de (Coord.). *Direito & Internet III – Tomo I: Marco Civil da internet (Lei n. 12956/2014)*. São Paulo: QuartierLatin, 2015.p.263-290.

LOJKINE, Jean. *A revolução informacional*. Tradução de José Paulo Netto. 3 ed. São Paulo: Cortez, 2002.

MARCEL, Leonardi. *Dados pessoais, regulação e a economia digital.* Disponível em: <http://leonardi.adv.br/2011/03/dados-pessoais-regulacao-e-a-economia-digital/>. Acesso em: 13 fev. 2017.

_____; *Tutela e privacidade na internet.* São Paulo: Saraiva 2011.

MACHADO, Joana de Souza; NEGRI, Sergio M. C. A. Direito, dignidade humana e o lugar da justiça: uma análise da utopia realista de Habermas. In: *Revista Brasileira de Estudos Políticos*. Belo Horizonte, n. 103, jul/dez 2011.
Disponível em:<http://www.pos.direito.ufmg.br/rbepdocs/103183204.pdf>. Acesso em: 13 fev. 2017.

MARTINS-COSTA, Judith. *Pessoa, personalidade, dignidade (ensaio de uma qualificação*). 2003. Tese (livre-docência em Direito Civil), Congregação da Faculdade de Direito, Universidade de São Paulo, São Paulo, 2003.

MATTELART, Armand. *Sociedade do conhecimento e controle da informação e da comunicação*. Conferência proferida na sessão de aberta do V Encontro Latino de Economia Política da Informação, Comunicação e Cultura, realizada em Salvador, de 09 a 11 de novembro de 2005. Disponível em:
<http://www.gepicc.ufba.br/enlepicc/ArmandMattelartPortugues.pdf>. Acesso em: 13 fev. 2017.

MENDES, Gilmar Ferreira. *Direitos fundamentais e controle de constitucionalidade: estudos de Direito Constitucional*. 3. ed., rev. e ampl. São Paulo: Saraiva, 2004.

_____; BRANCO, Paulo Gustavo Gonet. *Curso de direito constitucional*. 7. ed. rev. e atual. São Paulo: Saraiva, 2012.

MENDES, Laura Schertel. O Direito fundamental à proteção de dados pessoais. *Revista de Direitos do Consumidor*, São Paulo, ano 20, n. 79. 2011.

_____; DONEDA, Danilo. Marco jurídico para a cidadania digital: uma análise do projeto de lei 5.276/2016. *Revista de Direito Civil Contemporâneo*, São Paulo, vol. 09, ano 03, p. 35-48, out.-dez. /2016.

_____. A Tutela da Privacidade do Consumidor na Internet: Uma Análise à Luz do Marco Civil da Internet e do Código de Defesa do Consumidor. In: LUCCA, Newton de;

FILHO, Adalberto Simão; LIMA, Cíntia Rosa Pereira de (Coord.). *Direito & Internet III – Tomo I: Marco Civil da internet (Lei n. 12956/2014)*. São Paulo: QuartierLatin, 2015.p. 471 – 502.

MIRANDA, Rosângelo Rodrigues de. *A proteção constitucional da vida privada.* São Paulo, LED, 1996.

MONTEIRO, Renato Leite. *A nova regulação de proteção de dados pessoais aprovada na União Europeia e sua influência no Brasil*. Disponível em: <http://renatoleitemonteiro.com.br/analises-juridicas/a-nova-regulacao-de-protecao-de-dados-pessoais-aprovada-na-uniao-europeia-e-sua-influencia-no-brasil/>. Acesso em: 13 fev. 2017.

MORENO, José Carlos. *A internet em McLuhan, Baudrillard e Habermas*. Observatório Jornal, vol. 7, n. 03 (2013). Disponível em: <http://obs.obercom.pt/index.php/obs/article/viewFile/697/624>. Acesso em: 13 defevereiro de 2017.

MORAES, Maria Celina Bodin de. *Ampliando os direitos da personalidade. Na medida da pessoa humana: Estudos de direito civil-constitucional*. Rio de Janeiro: Renovar, 2010. Disponível em: <https://www.academia.edu/9689598/Ampliando_os_direitos_da_personalidade>. Acesso em: 13 fev. 2017.

MULHOLLAND, Caitlin. O Direito de não saber como decorrência do direito à intimidade – Comentário ao REsp 1.195.995. Civilistica.com. Rio de Janeiro, a. 1, n. 1, jul.-set./2012. Disponível em: <http://civilistica.com/wp-content/uploads/2012/09/Direito-de-nao-saber-civilistica.com-1.-2012.pdf>. Acesso em: 13 fev. 2017.

NEGRI, Sérgio Marcos Carvalho de Ávila. As razões da pessoa jurídica e a expropriação da subjetividade. *Civilistica.com.* Rio de Janeiro, a. 5, n. 2, 2016. Disponível em: <http://civilistica.com/wp-content/uploads/2016/12/Negri-civilistica.com-a.5.n.2.2016.pdf.>. Acesso em 13 fev. 2017.

PARENTONI, Leonardo Netto. O Direito ao Esquecimento (RighttoOblivion). In: LUCCA, Newton de; FILHO, Adalberto Simão; LIMA, Cíntia Rosa Pereira de (Coord.). *Direito & Internet III – Tomo I: Marco Civil da internet (Lei n. 12956/2014)*. São Paulo: Quartier Latin, 2015.p.539-618.

PEZZELLA, Maria Cristina Cereser; GHISI, Silvano. Privacidade na sociedade da informação: controle e direito ao esquecimento em espaços públicos. *Revista da AJURIS,* v. 40, n. 132, p. 231-258, dez./2013.Disponível em: <http://www.ajuris.org.br/OJS2/index.php/REVAJURIS/article/view/257/192>. Acesso em: 13 fev. 2017.

PODESTA, Fábio Henrique. Marco Civil da Internet e Direitos da Personalidade.In: LUCCA, Newton de; FILHO, Adalberto Simão; LIMA, Cíntia Rosa Pereira de (Coord.). *Direito & Internet III – Tomo I: Marco Civil da internet (Lei n. 12956/2014)*. São Paulo: Quartier Latin, 2015.p.385-404.

REGULATION (EU) No XXX/2016 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Disponível em: <https://iapp.org/media/pdf/resource_center/2015_12_15-GDPR_final_outcome_trilogue_consolidated_text.pdf>. Acesso em: 13 fev. 2017.

RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

_____. Transformações do corpo. *Revista Trimestral de Direito Civil*, vol. 19. Rio de Janeiro: jul./set. 2004, p. 91-107.

_____. Por que é necessária uma Carta de Direitos da Internet? Trad. Bernardo Diniz Accioli de Vasconcellos e Chiara Spadaccini de Teffé. *Civilistica.com*. Rio de Janeiro, a. 4, n. 2, jul./dez.2015. Disponível em: <http://civilistica.com/wp-content/uploads/2015/12/Rodota%CC%80-trad.-de-Teffe%CC%81-e-Vasconcellos-civilistica.com-a.4.n.2.20152.pdf>. Acesso em: 13 fev. 2017.

SAMPAIO, Rafael Cardoso; BARROS, Chalini Torquato Gonçalves de. Internet como esfera pública? Análise de usos e repercussões reais das discussões virtuais. *Estudos em Comunicação*, Covilhã, Portugal, n. 09, p. 161-183, maio 2011. Disponível em: <http://www.ec.ubi.pt/ec/09/pdf/EC09-2011Mai-09.pdf>. Acesso em: 13 fev. 2017.

SANTOS, Plácida Leopoldina Ventura Amorim da Costa; CARVALHO, Angela Maria Grossi de. Sociedade da informação: avanços e retrocessos no acesso e no uso da informação. *Revista Informação & Sociedade: Estudos*, João Pessoa, v.19, n.1, p. 45-55, jan./abr. 2009. Disponível em: <http://www.ies.ufpb.br/ojs/index.php/ies/article/viewFile/1782/2687>. Acesso em: 13 fev. 2017

SARLET, Ingo Wolfgang. As dimensões da dignidade da pessoa humana: construindo uma compreensão jurídico-constitucional necessária e possível. *Revista Brasileira de Direito Constitucional – RBDC*, n. 09, p. 361-388, jan./jun. 2007

SOMBRA, Thiago Luis. Rumos da agenda de proteção de dados e da privacidade na Internet. *UNB Notícia*, jul. 2016. Disponível em: <http://www.noticias.unb.br/artigos-main/808-os-rumos-da-agenda-de-protecao-de-dados-e-da-privacidade-na-internet>. Acesso em: 13 fev. 2017.

SILVA, José Afonso da. *Curso de direito constitucional positivo*. 32. ed. São Paulo: Malheiros, 2009.

STANCIOLI, Brunello. *Renúncia ao exercício de direitos da personalidade*. Belo Horizonte: Del Rey,2010.

SVALOV, Bárbara. O direito à informação e a proteção dos direitos de personalidade. In: GOZZO, Débora (Coord.). *Informação e direitos fundamentais*: a eficácia horizontal das normas constitucionais. São Paulo: Saraiva, 2012.

TEFFÉ, Chiara Antonia Spadaccini de. *A existência refletida: o direito à imagem a partir de uma perspectiva civil-constitucional*. In: REZENDE, Elcio Nacur; RODRIGUES JUNIOR, Otávio Luiz; OLIVEIRA, José Sebastião de (Coord.). Direito civil contemporâneo. Florianópolis: CONPEDI, 2015.

TOFFLER, Alvin. *A terceira onda*. 23. ed. São Paulo: Record, 1998.

UNIÃO EUROPEIA. Carta dos Direitos Fundamentais da União Europeia (2000). *ParlamentoEuropeu, Conselho da União Europeia e Comissão Europeia*. Disponível em: <http://www.fd.uc.pt/CI/CEE/pm/Tratados/Nice/Carta%20Direitos%20Fundamentais.pdf>. Acesso em: 13 fev. 2017.

_____. Diretiva1995/46CE, de 24 de outubro de 1995. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. *Diário Oficial das Comunidades Europeias*, Bruxelas, 31 jul.2002. Disponível em: <http://eur-http://eur-lex.europa.eu/pt/index.htm>.Acesso em: 13 fev. 2017.

_____. Diretiva 2002/58 CE, de 12 de dezembro de 2002. Relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrônicas (Diretiva relativa à privacidade e às comunicações eletrônicas). *Diário Oficial das Comunidades Europeias*, Bruxelas, 31 jul.2002. Disponível em: <fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-pt.pdf>.Acesso em:13 de fevereiro de 2017.

UNITED STATES. Department of health, education, and welfare. *Records, computers and the right of citizens*. July 1973. Disponível em: <https://www.justice.gov/opcl/docs/rec-com-rights.pdf>. Acesso em: 13 fev. 2017.

VIEIRA, Tatiana Malta. *O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação*. Porto Alegre: Sérgio Antônio Fabris, 2007.

WARREN, Samuel; BRANDEIS, Louis. ”The right to privacy”, in: *Harvad Law Review 193.* 1890. Disponível em: <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr_fn.html#fn0>. Acesso em: 13 fev. 2017.

ZANATTA, Rafael A. F. A Proteção de Dados Pessoais entre Leis, Códigos e Programação: Os Limites do Marco Civil da Internet. In: LUCCA, Newton de FILHO, Adalberto Simão; LIMA, Cíntia Rosa Pereira de (Coord.). *Direito & Internet III – Tomo I: Marco Civil da internet (Lei n. 12956/2014)*. São Paulo: Quartier Latin, 2015.p. 447- 470.