UNIVERSIDADE FEDERAL DA BAHIA
FACULDADE DE DIREITO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

BRUNO RICARDO DOS SANTOS PASSOS

O DIREITO À PRIVACIDADE E A PROTEÇÃO AOS DADOS PESSOAIS NA SOCIEDADE DA INFORMACÃO: UMA ABORDAGEM ACERCA DE UM NOVO DIREITO FUNDAMENTAL

Salvador
2017

BRUNO RICARDO DOS SANTOS PASSOS

O DIREITO À PRIVACIDADE E A PROTEÇÃO AOS DADOS PESSOAIS NA SOCIEDADE DA INFORMACÃO: UMA ABORDAGEM ACERCA DE UM NOVO DIREITO FUNDAMENTAL

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade Federal da Bahia, como requisito final para obtenção do Título de Mestre em Direito Público, sob orientação do Prof. Dr. Ricardo Maurício Freire Soares.

Salvador
2017

PASSOS, Bruno Ricardo dos Santos
O direito à privacidade e a proteção aos dados pessoais na sociedade da informação: uma abordagem acerca de um novo direito fundamental. / Bruno Ricardo dos Santos PASSOS. -- Salvador, 2017.
102 f.

Orientador: Ricardo Maurício Freire SOARES.
Dissertação (Mestrado - Faculdade de Direito) -- Universidade Federal da Bahia, Universidade Federal da Bahia, 2017.

1. Direito à Privacidade. 2. Proteção aos Dados Pessoais. 3. Marco Civil da Internet. I. SOARES, Ricardo Maurício Freire. II. Título.

BRUNO RICARDO DOS SANTOS PASSOS

O DIREITO À PRIVACIDADE E A PROTEÇÃO AOS DADOS PESSOAIS NA SOCIEDADE DA INFORMACÃO: UMA ABORDAGEM ACERCA DE UM NOVO DIREITO FUNDAMENTAL.

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade Federal da Bahia, como requisito final para obtenção do título de Mestre em Direito Público, Programa de Pós-Graduação da Faculdade de Direito, Universidade Federal da Bahia.

Aprovada em 23 de março de 2017.

Prof. Dr. Ricardo Maurício Freire Soares _____

Pós-Doutor em Direito pela Universitá degli Studi di Roma La Sapienza.

Doutor em Direito Público pela Universidade Federal da Bahia.

Prof. Dr. Saulo José Casali Bahia _____

Doutor em Direito pela Pontifícia Universidade Católica de São Paulo.

Prof. Dr. Valdir Ferreira de Oliveira Junior _____

Doutor em Direito Público pela Universidade Federal da Bahia.

AGRADECIMENTOS

Agradeço a Deus pela oportunidade, bem como à minha mãe Zélia pelas valiosas orientações e dedicado empenho na tarefa materna.

Ao meu pai Carlos e aos meus irmãos Marco, Fábio e Talita pela compreensão diante das minhas ausências em razão da vida acadêmica.

Agradeço imensamente à minha esposa Iana pelo amor, apoio e companheirismo que foram fundamentais à conclusão deste trabalho.

À equipe do Programa de Pós-graduação em Direito desta Universidade, pelo auxílio e apoio no desenvolvimento de toda a pós-graduação.

Ao Prof. Dr. Ricardo Maurício Freire Soares, orientador deste trabalho, pela confiança e pelo respeito que se fizeram presentes em nosso convívio.

Agradeço também aos professores da UFBA, aos colegas de curso e aos amigos que, direta ou indiretamente, incentivaram minha jornada.

Agradeço ainda à FAPESB – Fundação de Amparo à Pesquisa do Estado da Bahia, pelo auxílio no cumprimento deste objetivo, ao investir na pesquisa e fomentar o desenvolvimento acadêmico.

A todos, os de perto e os de longe, que de alguma maneira contribuíram para a conclusão deste trabalho.

A liberdade de expressão não é um direito absoluto, nem ilimitado.

Nenhum direito fundamental o é.

(KOATZ, 2011, p. 401)

PASSOS, Bruno Ricardo dos Santos. O direito à privacidade e a proteção aos dados pessoais na sociedade da informação: uma abordagem acerca de um novo direito fundamental. 102 f. 2017. Dissertação (Mestrado) – Faculdade de Direito, Universidade Federal da Bahia, Salvador, 2017.

RESUMO

O século XXI é marcado pelo avanço tecnológico e pela relativização das barreiras territoriais das nações. O processo da globalização permitiu uma maior integração entre os povos, sobretudo após o surgimento do computador e da internet. Diante da moderna sociedade da informação, oriunda do grande avanço tecnológico jamais experimentado em épocas anteriores, a vida privada do indivíduo parece estar sendo ameaçada, haja vista as inúmeras ferramentas de controle comportamental disponíveis no mercado de consumo, a exemplo das câmeras de vigilância e *webcams*, dos drones, do monitoramento do fluxo de dados na internet, dos *smartphones*, das mídias sociais, dentre outros. Neste sentido, mostra-se necessário assegurar ao indivíduo instrumentos legais para a garantia da privacidade e do controle sobre os dados pessoais. A pesquisa apresenta como objetivo verificar na literatura brasileira e estrangeira como o direito à privacidade vem sendo abordado no contexto da proteção aos dados pessoais dos indivíduos, frente aos impactos de uma sociedade da informação e do consumo. A pesquisa fora pautada na revisão da literatura existente acerca da proteção da privacidade e do controle sobre os dados pessoais dos indivíduos, adotando-se um método dedutivo e sistemático, partindo da perspectiva do direito comparado, através do estudo das experiências do ordenamento jurídico europeu e norte-americano, para então desaguar na abordagem específica do direito brasileiro. A pesquisa evidencia que, ainda que se trate de um tema muito recente no Brasil, os diplomas vigentes parecem não serem suficientes para se atribuir ao indivíduo o controle efetivo sobre os seus próprios dados pessoais, sobretudo porque a internet é uma tecnologia transnacional.

Palavras-chave: Direito à Privacidade. Proteção aos Dados Pessoais. Marco Civil da Internet.

PASSOS, Bruno Ricardo dos Santos *The right to privacy and protection of personal data in the information society*: *an approach to a new fundamental right*. 102 pp. 2017. *Master Dissertation* - Faculdade de Direito, Universidade Federal da Bahia, Salvador, Bahia, *Brazil*, 2017.

ABSTRACT

The 21st century is marked by technological advances and by the relativization of the territorial barriers of nations. The process of globalization allowed for greater integration among peoples, especially after the emergence of the computer and the internet. In the face of the modern information society, stemming from the great technological advance never experienced in previous times, the private life of the individual seems to be threatened, given the innumerable behavioral control tools available in the consumer market, such as surveillance cameras and webcams, Drones, data flow monitoring on the internet, smartphones, social media, among others. In this sense, it is necessary to assure the individual legal instruments for the guarantee of privacy and control over personal data. The research aims to verify in the Brazilian and foreign literature how the right to privacy has been approached in the context of the protection of the personal data of individuals, against the impacts of an information society and consumption. The research was based on a review of the existing literature on the protection of privacy and control of personal data of individuals, adopting a deductive and systematic method, from the perspective of comparative law, through the study of the experiences of the European legal order and American, and then to embark on the specific approach of Brazilian law. The research shows that, although it is a very recent issue in Brazil, the current diplomas seem not to be enough to give the individual effective control over their own personal data, especially since the Internet is a transnational technology.

Keywords*: Right to Privacy. Protection of Personal Data. Civil Landmark of the Internet.*

LISTA DE ABREVIATURAS

CC	Código Civil
CDC	Código de Defesa do Consumidor
CE	Convenção Européia
CF	Constituição Federal
CFJ	Conselho da Justiça Federal
CPPA	*Consumer Privacy Protection Act*
DPPA	*Driver's Privacy Protection Act*
DUDH	Declaração Universal dos Direitos Humanos
FCRA	*Fair Credit Reporting Act*
FERPA	*Family Educational Rights and Privacy Act*
FOIA	*Freedom of Information Act*
FPA	*Financial Privacy Act*
GLBA	*Gramm-Leach-Bliley Act*
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
OLAP	*Online Analytical Processing*
ONU	Organização das Nações Unidas
PET	*Privacy Enhancing Technologies*
STJ	Superior Tribunal de Justiça
VPPA	*Video Privacy Protection Act*

SUMÁRIO

1 INTRODUÇÃO

O século XX é marcado pelo avanço tecnológico e pela relativização das barreiras territoriais das nações. O processo da globalização permitiu uma maior integração entre os povos, sobretudo após o surgimento do computador e da internet. A informação nunca se difundiu de forma mais rápida, e um acontecimento ocorrido em uma parte do globo logo chega ao conhecimento dos demais indivíduos.

É o contexto de surgimento da sociedade da informação, caracterizada pela criação de ferramentas que favorecem a difusão do conhecimento e da comunicação entre os povos, aproximando línguas, culturas e tradições. Entretanto, verifica-se que esta sociedade é dinâmica e complexa, sempre evidenciando o potencial de expansão e readaptação com os valores cultuados pela comunidade.

Diante da moderna sociedade da informação, gestada em decorrência do grande avanço tecnológico jamais experimentado em épocas anteriores, a vida privada do indivíduo parece ter sido ameaçada, haja vista as inúmeras ferramentas de controle comportamental disponíveis no mercado de consumo, a exemplo das câmeras de vigilância e *webcams*, dos drones, dos *smartphones*, das mídias sociais, dentre outros.

De acordo com Manuel Castells, a sociedade contemporânea se depara com uma revolução tecnológica, cuja essência está pautada nos sistemas de informação, de processamento e de comunicação (CASTELLS, 1999, p. 50). Em que pese o desenvolvimento trazido por esta expansão, a privacidade dos indivíduos passou a ser relativizada, sobretudo no que se refere à proteção aos dados pessoais, uma nova perspectiva da privacidade surgida no século XX.

Diante desta conjuntura, surgem questionamentos relevantes: o direito à proteção dos dados pessoais vem sendo garantido pelo ordenamento jurídico mundial? Há uma norma específica a tratar sobre o tema no Brasil? Acaso a resposta tenha sido positiva, tais normas se mostram suficientes para a efetiva garantia deste direito diante da sociedade moderna?

Desta forma, esta pesquisa está direcionada à hipótese de que a proteção aos dados pessoais é uma tutela que vai além da privacidade e que, no caso do Brasil, as normas jurídicas existentes não se mostram suficientes para uma implementação efetiva deste direito fundamental.

Como método de trabalho, se utilizou a revisão de literatura inerente à proteção da privacidade e ao controle sobre os dados pessoais dos indivíduos, adotando-se um método dedutivo e sistemático, mediante o qual se partiu de uma perspectiva mais ampla representada no direito comparado pelas experiências do ordenamento jurídico europeu e norte-americano para então desaguar na abordagem específica do direito brasileiro.

Para tanto, após esta seção introdutória, a presente dissertação é composta de mais quatro seções e suas respectivas divisões para a compreensão do tema. Na segunda seção, se aborda o **Direito à vida privada como um direito da personalidade**, elencando o seu objeto e suas características fundamentais, perpassando pela análise da teoria das esferas de proteção até o estudo da correlação entre a privacidade, a dignidade da pessoa humana e a proteção aos dados pessoais.

Na terceira seção a abordagem é sobre **Os dados pessoais e a sociedade de consumo** e tem como objeto de discussão o contexto de surgimento da sociedade da informação e do consumo, sobretudo em decorrência da grande influência da internet e da globalização, abordando as técnicas frequentes adotadas atualmente para a coleta e o tratamento dos dados pessoais.

A quarta seção desenvolve **A proteção dos dados pessoais no direito comparado,** descrevendo a origem da sua proteção no cenário internacional, na comunidade europeia e no direito norte-americano, partindo de uma análise comparativa de algumas das experiências vigentes no continente europeu, integrante da tradição romano-germânica também composta pelo Brasil, e também da experiência ocorrida na *common law* dos Estados Unidos.

Na quinta e última seção descreve **A tutela dos dados pessoais no direito brasileiro** onde está traçada uma abordagem específica da correlação entre a proteção aos dados pessoais e o direito brasileiro, iniciando com um retrato da sua tutela enquanto um direito fundamental e da existência de alguns instrumentos infraconstitucionais para a garantia do direito à privacidade e ao sigilo quanto aos dados pessoais, partindo do Código de Defesa do Consumidor até o Marco Civil da Internet e sua consequente regulamentação.

2 O DIREITO À VIDA PRIVADA COMO UM DIREITO DA PERSONALIDADE

2.1 CONCEITO E OBJETO DOS DIREITOS DA PERSONALIDADE

Quando se tratam dos direitos da personalidade, refere-se ao catálogo de garantias fundamentais que são inerentes ao indivíduo e que contemplam os aspectos mais reservados da sua existência em sociedade, com uma íntima correlação com a tutela da privacidade.

Tratam-se de direitos vitais haja vista que são responsáveis pela identificação e individualização das características de um determinado cidadão, sendo fundamentais para o adequado convívio social. E, neste sentido, atuando a disciplina jurídica como reguladora do comportamento social, também lhe cabe atuar como um árbitro na atribuição da personalidade.

Embora desde o surgimento do Cristianismo já houvesse registro da tutela aos direitos humanos, o reconhecimento da proteção dos direitos da personalidade enquanto um direito subjetivo é uma construção recente, que sofreu influência direta da Revolução Francesa e da Declaração dos Direitos do Homem de 1789, bem como do período posterior às Duas Grandes Guerras com o surgimento da Organização das Nações Unidas em 1948 e, ainda, em decorrência da vigência da Convenção Europeia de 1950.

Conforme nos esclarece Adriano de Cupis (2008, p.19-21), a personalidade jurídica, também nomeada como capacidade jurídica, pode ser definida como a "susceptibilidade de ser titular de direitos e obrigações jurídicas". Neste sentido, não teria identificação nem com os direitos nem com as obrigações, manifestando-se apenas como uma qualidade jurídica, constituindo apenas de uma "precondição", ou, melhor esclarecendo, o seu fundamento e pressuposto.

No mesmo sentido é a doutrina de Carlos Alberto Bittar (2006, p. 5), que nos acrescenta que os direitos da personalidade são aqueles inerentes à pessoa em função da estruturação física, mental e moral que lhes são próprias. E por conta desta função, seriam dotados de características peculiares que lhe conferem o status da singularidade na seara do direito privado, sobretudo os aspectos da intransmissibilidade e da sua irrenunciabilidade, que se projetam em garantias contra a ação lesiva do próprio titular.

O entendimento dominante é no sentido de que os direitos da personalidade não precisariam estar expressos no plano do direito positivo de qualquer nação, haja vista refletirem-se em direitos inatos, cabendo ao Estado a simples tarefa de declará-los enquanto direitos fundamentais e sancionar a conduta contrária (BITTAR, 2006, p. 7).

Entretanto, a dinâmica das sociedades modernas exigiu a expressa positivação destes direitos personalíssimos, auferindo proteção tanto em nível constitucional como em infraconstitucional aos indivíduos, seja contra o arbítrio do próprio Estado no afã do controle social, sejam contra as incursões arbitrárias dos particulares.

Adriano de Cupis (2008, p. 23-24) entende que todos os direitos poderiam ser chamados de "direitos da personalidade", haja vista que todos estariam destinados a dar conteúdo à personalidade. Entretanto, para a doutrina jurídica, sobretudo as dos países de origem romano-germânica, em uma visão generalista e tecnicamente pouco precisa, a designação dos "direitos da personalidade" estaria reservada apenas aos direitos subjetivos.

Contudo, considerando a importância da sua carga valorativa, o fato marcante para a ampliação da proteção dos direitos da personalidade surgiu com a promulgação da Constituição Federal do Brasil de 1988, que, de forma expressa no art. 5º, inciso X, assegurou a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, garantindo a tutela indenizatória inerente na hipótese de sua violação.

Neste sentido, o objeto dos direitos da personalidade, verdadeiro direito fundamental, é revestido de um caráter de proeminência quando sopesados com outros direitos fundamentais assessórios. Este objeto apresentaria duas características que o identificam: a primeira consiste na sua intrínseca correlação com os interesses mais privados do indivíduo; o segundo os identifica como os bens jurídicos de maior valor a serem tutelados pela sociedade. (CUPIS, 2008, p. 29).

Todo indivíduo necessita de uma seara de proteção da sua intimidade e da sua vida privada, de modo que possa desenvolver as capacidades físicas e psíquicas que o possibilitem desenvolver a sua autonomia em sociedade. E desta forma, o objeto dos direitos da personalidade não é exterior ao sujeito de direito, ao contrário de outros bens jurídicos tutelados pelo ordenamento de uma nação.

Cabe ainda evidenciar que existe uma pluralidade de direitos da personalidade. Não se trata de interesses taxativos e protegidos em *numerus clausus* pelos ordenamentos positivos. Em que pese à norma constitucional brasileira, criada no contexto histórico, político, social e

econômico de 1988 apenas tenham enumerado expressamente a intimidade, a vida privada, a honra e a imagem como direitos da personalidade, não deixou de fora da tutela os diversos outros direitos personalíssimos implícitos, como a proteção do nome, a integridade física ou a garantia de proteção da privacidade no meio digital, realidade tecnológica da nossa sociedade moderna.

Defendendo a tese da pluralidade dos direitos da personalidade, Adriano de Cupis acrescenta:

> Recorde-se que deixamos atrás admitido que a individualização do bem resulta da individualização das necessidades; que a exigência é distinta da liberdade, e que a necessidade de vivermos respeitados, não se confunde com a necessidade de nos distinguirmos das outras pessoas. De tudo isto deriva que são também distintos os bens correspondentes, e bem assim os direitos sobre estes. (2008, p. 32).

De tudo o que acaba de ser exposto, resulta que os direitos da personalidade constituem uma categoria autônoma no sistema dos direitos subjetivos, pois "só nas mais vastas categorias dos direitos subjetivos (direitos privados, não-patrimoniais, absolutos) podemos integrar os direitos da personalidade; em nenhuma das outras que naquelas se contém podem ser incluídos." (CUPIS, 2008, p. 38). Discorda-se apenas no que tange ao suposto caráter absoluto dos direitos fundamentais, incompatível com o entendimento da doutrina jurídica contemporânea.

Podemos dividir os direitos da personalidade em duas categorias distintas: inatos ou adquiridos. Na primeira hipótese podemos exemplificar com o direito à vida e à integridade física e moral; já no que tange aos direitos adquiridos, seriam todos aqueles que decorreriam em consequência do *status* individual assegurado pelo ordenamento jurídico.

A escola positivista rejeita a tese de que os direitos da personalidade sejam inatos, tais como refere Adriano de Cupis. Segundo o autor, "[...] não é possível denominar os direitos da personalidade como "direitos inatos", entendidos no sentido de direitos relativos, por natureza, à pessoa." (CUPIS, 2008, p. 25).

Os direitos inerentes à personalidade do indivíduo, diante do seu caráter de essencialidade, podem ser considerados na maioria das vezes como direitos inatos, entretanto, não se reduzem a este âmbito de compreensão. Todo direito inato será considerado um direito da personalidade, contudo, podem ser identificadas hipóteses de direitos que passaram a ser entendidas como personalíssimas, mas "não têm por base o simples pressuposto da personalidade, e que, todavia, *uma vez revelados*, adquirirem caráter de essencialidade"

(CUPIS, 2008, p. 27). Pode-se exemplificar com a hipótese de extensão dos direitos da personalidade às pessoas jurídicas.

É importante ainda mencionar que apesar da grande variedade de direitos que integram a seara personalíssima do sujeito, nem todos que o integram seriam compatíveis com todo e qualquer sujeito de direito. Apesar da Teoria do Direito estender artificialmente às pessoas jurídicas a característica de ser um "sujeito de direito", e, portanto, de direitos inerentes à personalidade, nem todos eles são aplicáveis, haja vista a íntima correlação do instituto com as necessidades essenciais da pessoa humana.

A compreensão mais adequada, salvo melhor juízo, seria aquela de que o objeto da personalidade não pode ser satisfeito na integralidade, seja de ordem física ou moral, entre as pessoas físicas e jurídicas. Neste mesmo sentido é o entendimento de Adriano de Cupis (2008, p. 33) quando esclarece que "a personalidade [...], na mesma medida em que respeita às pessoas físicas, encontra limitação na essência mesma das pessoas jurídicas, cujo substrato natural difere profundamente do das pessoas físicas."

Uma vez evidenciados o conceito, o objeto e algumas noções fundamentais sobre os direitos da personalidade, oportuno o aprofundamento do tema com a menção às suas características fundamentais.

2.2 CARACTERÍSTICAS DOS DIREITOS DA PERSONALIDADE

Os direitos da personalidade são aqueles vitais para a identificação e a individualização das características de um determinado indivíduo, sendo fundamentais para o adequado convívio social. E, nesta perspectiva, podemos compreender que a personalidade inclui-se entre os direitos de cunho não-patrimonial.

Em que pese o direito da personalidade não tenha na sua essência um caráter patrimonial, isto não significa que na hipótese de violação de um direito da personalidade não se esteja sujeito a uma indenização de cunho patrimonial. Como bem evidenciou Adriano de Cupis (2008, p. 37), "o caráter patrimonial do direito derivado da indenização pelo dano não pode alterar o caráter não-patrimonial dos direitos da personalidade."

Conforme Carlos Alberto Bittar (2006, p. 17), pode-se classificar e distribuir os direitos da personalidade em três categorias que se complementam. São direitos físicos,

porque a tutela alcança a estrutura física do indivíduo, quando, por exemplo, se protege a integridade corporal, nela incluídos os órgãos, os membros, a imagem, etc.

São também os direitos psíquicos, porque se relacionam com o desenvolvimento da personalidade do ser humano, compreendendo a tutela da liberdade, da intimidade, do sigilo, etc. Aqui se inclui a proteção à privacidade dos dados pessoais gerados pelo uso da internet ou de qualquer outra ferramenta tecnológica exigida no mundo moderno.

A terceira categoria é aquela que identifica alguns dos direitos da personalidade como direitos morais. São assim rotulados porque se relacionam com as virtudes ou os atributos axiológicos do indivíduo em sociedade, tais como a identidade, o honra ou qualquer outra manifestação benéfica do intelecto.

De acordo com a previsão do art. 11 do Código Civil, com "exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária". (BRASIL, 2002).

Da leitura do artigo supracitado se extraem algumas das principais características dos direitos da personalidade. Para Carlos Alberto Gonçalves (2012, p. 187), ainda poderia se acrescentar serem absolutos, ilimitados, imprescritíveis, impenhoráveis, inexpropriáveis e vitalícios.

Uma das características dos direitos da personalidade, em conformidade com o diploma civilista, é a sua *intransmissibilidade*. Esta reside na natureza do objeto, que constitui uma carga valorativa de tamanha importância ao indivíduo que assume uma posição de destaque, inclusive contra a própria atuação autolesiva do titular na hipótese de tentar aliená-lo ou transmiti-lo a terceiros. Logo, a vida, a integridade, a honra ou a privacidade de alguém, por exemplo, não podem ser transferidos a outrem.

A intransmissibilidade acarreta a plena indisponibilidade dos direitos da personalidade, não podendo o seu titular deles dispor, transmiti-lo a terceiros, renunciar o seu uso, muito menos abandoná-lo, haja vista que surgem e se extinguem com o indivíduo, dele integrando partes inseparáveis. De acordo com Adriano de Cupis (2008, p. 58), "os direitos da personalidade estão subtraídos à disposição individual, tanto como a própria personalidade".

Entretanto, cabe reafirmar que a indisponibilidade dos direitos da personalidade não pode ser considerada absoluta, à medida que alguns deles possibilitam cessão para fins comerciais, a exemplo do direito à imagem e do direito autoral. Por conseguinte, o produto da

exploração de algum destes direitos, ou seja, o benefício pecuniário pode ser penhorado, mas não o direito em si.

Seguindo esta mesma orientação, o Conselho da Justiça Federal propõe o Enunciado 4 da I Jornada de Direito Civil, onde prevê em seu art. 11 que "O exercício dos direitos da personalidade pode sofrer limitação voluntária, desde que não seja permanente nem geral". (BRASIL, 2012).

Aclarando ainda mais a situação, o Superior Tribunal de Justiça decidiu que "O direito de ação por dano moral é de natureza patrimonial e, como tal, transmite-se aos sucessores da vítima" (RSTJ, 71/183). Daí decorre a compreensão de que ainda que sejam considerados personalíssimos e intransmissíveis os direitos da personalidade, a eventual pretensão indenizatória contra sua violação é passível de transmissão, na forma como autoriza o art. 943 do Código Civil (BRASIL, 2002).

Outra característica dos direitos da personalidade é a sua *irrenunciabilidade*. A faculdade de renunciar é diretamente associada à capacidade de dispor de determinado direito, logo, quando um direito é indisponível será ele também irrenunciável. Esta característica se justifica pela essencialidade do conteúdo, cujo titular dele não pode dispensar.

A personalidade se esvaziaria se fosse autorizado ao titular pôr fim a tais direitos por ato voluntário. De certo, o ato de renúncia não poderia fulminar os atributos necessários ao desenvolvimento da autonomia plena do indivíduo, haja vista que "a norma jurídica, ao atribuir os direitos da personalidade, tem caráter de norma de ordem pública, irrevogável". (CUPIS, 2008, p. 59-60). Desta forma, são interesses que devem permanecer necessariamente na esfera do próprio titular.

Além da indisponibilidade e da irrenunciabilidade, podemos elencar ainda o caráter *absoluto* dos direitos da personalidade, que atuam como consequência de serem oponíveis *erga omnes*. Os interesses tutelados são tão relevantes que são capazes de impor a todos indiscriminadamente um dever de abstenção e de obediência, ao passo que também são gerais porque inerentes a toda pessoa humana. (GONÇALVES, 2012, p. 188).

Entretanto, em que pese possamos reconhecer a grande relevância da proteção aos direitos fundamentais e também aos da personalidade, não parece adequado o entendimento de que haveria direitos absolutos. A implementação de todo e qualquer direito pressupõe a sua materialização através de políticas públicas, que necessariamente, exigem um aporte financeiro por parte do Estado. E não podemos negar que a sociedade moderna vive no

contexto real de que os recursos são escassos. Logo, poderá haver, em algum momento, um limite financeiro à implementação de um direito, por mais fundamental que seja.

Ademais, ainda que se afaste a discussão acerca da limitação financeira, não se pode perder de vista que o próprio legislador constituinte originário previu exceções aos direitos fundamentais, mesmo aqueles onde o bem jurídico seja mais relevante. O art. 5º, XLVII, "*a*" da Constituição Federal evidenciou o caráter relativo do direito à vida, ao menos na hipótese de guerra declarada. Neste sentido, nem mesmo os direitos da personalidade poderiam ser classificados como absolutos, o que também não pode servir de argumento para a desconsideração da sua garantia.

Em que pese o Código Civil, de 2002, nos seus artigos 11 a 21, tenham se referido textualmente a apenas alguns dos direitos da personalidade, podemos entender que estes também são caracterizados como *ilimitados*. A disposição legal referiu-se a um rol meramente exemplificativo e não em *numerus clausus*, haja vista ser impossível que possamos enumerar todos os direitos da personalidade passíveis de proteção. (GONÇALVES, 2012, p. 188).

Certo é que o Direito é o produto de uma conjuntura histórica de uma determinada época, de modo que o avanço econômico-social e científico pode vir a justificar em um futuro próximo a proteção de novos direitos da personalidade, até então não exemplificados pelo legislador originário.

Diante de grandes avanços tecnológicos tais como a internet, a clonagem e o monitoramento via satélite, "a personalidade passa a sofrer novas ameaças que precisarão ser enfrentadas, com regulamentação da sua proteção" (GONÇALVES, 2012, p. 189). Neste sentido, não restam dúvidas quanto à possibilidade de proteção da privacidade também no contexto dos dados pessoais do meio digital, haja vista refletir-se em uma nova realidade e também em novos perigos ao cidadão até então não imaginados pelo legislador constituinte.

Outra característica dos direitos da personalidade, sustentados por alguns autores é a sua *imprescritibilidade*. Trata-se de um atributo que assegura que tais direitos, considerando o seu conteúdo fundamental, não podem ser extintos pelo uso ou pelo decurso do tempo, tampouco pela inércia na pretensão de defendê-los. (GONÇALVES, 2012, p. 189).

A *impenhorabilidade* é mais uma das características importantes dos direitos da personalidade. Em sendo tais direitos inerentes à pessoa humana e dela indissociáveis e, por conseguinte, indisponíveis e irrenunciáveis, certamente não podem ser constritos, haja vista que a penhora é o ato de garantia forçada de um determinado bem a fim de satisfazer o

exequente. (GONÇALVES, 2012, p. 190). De certo, "à execução estão somente submetidos os direitos *patrimoniais transmissíveis*." (CUPIS, 2008, p. 65).

Carlos Alberto Gonçalves (2012, p. 190) ainda aponta que os direitos da personalidade teriam como característica a *vitaliciedade,* o que significaria que os mesmos seriam adquiridos no instante da concepção e extintos com a morte do titular. Entretanto, alguns desses direitos são resguardados mesmo após a morte, a exemplo do respeito ao morto, à sua honra ou à sua memória e ao seu direito moral de autor.

Neste sentido, estabelece o art. 12, parágrafo único do Código Civil de 2002 que, quando se trata de lesão a um direito da personalidade de um falecido, a legitimação para requerer a cessação da ameaça, lesão ou, ainda, a reparação pecuniária em sede de perdas e danos, é transferida ao "*cônjuge sobrevivente, ou qualquer parente em linha reta, ou colateral até o quarto grau*". (BRASIL, 2002).

De modo a esclarecer questões de ordem prática que frequentemente se deslocam ao judiciário, surge o Enunciado 275 da IV Jornada de Direito Civil realizada pelo Conselho da Justiça Federal, onde estabelece que "O rol dos legitimados de que tratam os artigos 12, parágrafo único, e 20, parágrafo único, do Código Civil, também compreende o companheiro". (BRASIL, 2012). Desta forma, houve a aplicação por analogia da legitimação do cônjuge.

Uma vez elencadas as características que identificam os direitos da personalidade, oportuna é a necessidade de se aprofundar a abordagem sobre a intimidade, a privacidade e o sigilo, mediante o estudo da teoria das esferas de proteção.

2.3 A TEORIA DAS ESFERAS DE PROTEÇÃO

A denominada Teoria das Esferas de Proteção, ou teoria dos círculos concêntricos da esfera da vida privada, surgiu na doutrina alemã do século XX, como um esforço para diferenciar o caráter público daquele diametralmente oposto: o privado.

Robert Alexy (2012, p. 360) chama a atenção para o fato de que a referida teoria das esferas de proteção surge da interpretação dada pelo Tribunal Constitucional Alemão, quando posto a decidir sobre o chamado *caso Elfes*. No referido acórdão, o Tribunal faz menção expressa a um "último e inviolável âmbito de liberdade humana".

Neste primeiro precedente histórico sobre o tema, a jurisprudência alemã difundiu a ideia de que a garantia da liberdade geral de ação pode ser almejada com o livre desenvolvimento da personalidade do indivíduo e, para tanto, estabeleceu algo que se pode representar como círculos concêntricos que delimitam os campos da personalidade onde, ao ponto central, sequer o Estado pode violar.

De acordo com Paulo José da Costa Junior (1995, p. 30-31) o homem vive sua vida cotidiana como personalidade em esferas diferenciadas, sendo uma delas a esfera individual, onde a tutela da personalidade se dá dentro da vida pública, e outra, a esfera privada, onde se protege a "inviolabilidade da personalidade dentro de seu retiro, necessário ao seu desenvolvimento e evolução, em seu mundo particular, à margem da vida exterior".

Estaria então delimitada a diferença entre a esfera individual situada na seara da proteção da honra, do nome e da reputação do sujeito de direitos, ao passo que no espaço da esfera privada materializariam os esforços para a proteção do titular contra a indiscrição, na sua intimidade e na sua individualidade. (COSTA JÚNIOR, 1995, p. 31-32).

Acrescenta o autor que esta mesma esfera da vida privada poderia ainda se ramificar em outras esferas de dimensões gradativamente inferiores, fato este que ocorre à medida que a intimidade se restrinja ainda mais. (COSTA JÚNIOR, 1995, p. 35). Trata-se da retratação gráfica de três esferas concêntricas, onde o ponto central seria o núcleo intangível, tanto pela atuação dos Estados ou pela ingerência de particulares.

É o que também se aufere das lições de Robert Alexy (2012, p. 360-361):

> É possível distinguir três esferas, com intensidade de proteção decrescente: *a esfera mais interior* (último e inviolável âmbito de liberdade humana), esfera íntima inviolável, (esfera nuclear da configuração da vida privada, protegida de forma absoluta), *a esfera privada ampliada*, que incluí o âmbito privado que não pertence à esfera mais interior, e a *esfera social*, que inclui tudo aquilo que não for atribuído nem ao menos à esfera privada ampliada.

Como mencionado, a primeira esfera, a mais ampla, é destinada ao campo de atuação da vida privada *stricto sensu*, onde contém aqueles acontecimentos que o cidadão não deseja que se tornem públicos. Em um grau de profundidade encontramos a segunda esfera, a que atinge a intimidade, ou a seara confidencial. Aqui restam excluídos tanto o grande público quanto aquelas pessoas conhecidas embora não íntimas.

Por derradeiro, no ponto central destes círculos concêntricos encontramos o núcleo intangível, o campo de proteção absoluto contra a indiscrição: a esfera do segredo. Aqui não

participam sequer as pessoas íntimas do sujeito de direitos, senão ele próprio. Trata-se do núcleo essencial da privacidade, pautado no princípio da dignidade humana, onde o indivíduo detém o sigilo necessário ao desenvolvimento da sua psique e consequentemente da personalidade.

Robert Alexy defende que a teoria das esferas poderia ser concebida como o resultado de sopesamento entre princípios colidentes, de um lado o princípio da liberdade negativa e, do outro, um conjunto de outros princípios. Acrescenta que nesta esfera mais interior da vida social, *per definitionem,* seria aquele onde os princípios fundamentais do indivíduo colidiriam. (ALEXY, 2012, p. 361).

Entretanto, cabe ponderar que a teoria das esferas de proteção enfrenta uma tendência moderna ao relativismo, estando ameaçada até mesmo a esfera mais fundamental, aquela destinada ao segredo do indivíduo. Quando nos referimos a um indivíduo que possui algum tipo de destaque social, ou seja, de caráter notório, o âmbito de atuação da sua vida privada tende a se restringir de forma bastante considerável.

No que tange às pessoas célebres, parece que a sua vida íntima seria objeto de maior interesse da coletividade, como se as personalidades pertencessem literalmente ao público e consentisse com alguma espécie de renúncia tácita à própria existência privada. Todavia, sempre deverá ser preservada uma parcela da intimidade, ainda que reduzida, também às personalidades midiáticas, "onde possam exprimir-se livremente, sem prestar contas a ninguém, abrigadas da curiosidade alheia". (COSTA JÚNIOR, 1995, p. 38-40).

Não é demais ponderar que esta esfera relativizada da intimidade das pessoas notórias é recuperada pelo artista que abandonou a sua carreira, ou pelo político que deixou a vida pública, ou, ainda pelo atleta que se aposentou da rotina de alto desempenho, recuperando a personalidade de que haviam se despojado anteriormente.

Ocorre que a curiosidade com as ocupações alheias é um fenômeno que vem cada vez mais se acentuado na sociedade moderna, pautada no avanço tecnológico. O desejo de conhecimento acerca de como os outros vivem alimenta uma verdadeira indústria da mídia, onde se circula muita riqueza como produto da exposição e venda de "informação" sobre as preferências e intimidades dos indivíduos, sobretudo das pessoas públicas.

Ocorre que esta realidade evidencia uma tendência de supressão da privacidade e da intimidade, passíveis de violação à dignidade da pessoa humana, princípio fundamental da República Federativa do Brasil.

2.4 A PRIVACIDADE E O PRINCÍPIO DA DIGNIDADE DA PESSOA HUMANA

Em sua evolução histórica, no pensamento filosófico da antiguidade clássica, por volta do século III a.C, a dignidade da pessoa humana era compreendida como a posição ocupada pelo indivíduo em uma sociedade e pelo grau do seu reconhecimento frente aos demais membros da comunidade. No pensamento estóico, a dignidade era assimilada como a qualidade que, por ser intrínseca ao ser humano, distinguia o mesmo das demais criaturas, evidenciando a noção de que todos os seres humanos eram dotados de igual dignidade. (SARLET, 2012, p. 34-35).

Diante da concepção dominante da religião cristã do século XIII, sobretudo pelo pensamento de Tomás de Aquino, o ser humano é assimilado à ideia de que fora gerado à imagem e semelhança do Criador, premissa que serviu de fundamento à compreensão de que o ser humano é dotado de um valor próprio e peculiar, não podendo ser tratado como objeto.

No âmbito do pensamento jusnaturalista do século XVII e XVIII, a concepção da dignidade da pessoa humana, assim como a ideia do direito natural em si passou por um processo de racionalização e laicização, mantendo-se, todavia, a noção fundamental, da igualdade de todos os homens em dignidade e liberdade.

Surgem os estudos de Immanuel Kant, que difundiu a noção de que o fundamento da dignidade da pessoa humana estaria relacionado com a capacidade da autonomia da vontade do indivíduo, definindo-a como a faculdade de agir de acordo com a previsão legal e de determinar a si próprio. (KANT, 1980, p. 104). O homem é visto como um ser racional e não como produto da disposição arbitrária de quaisquer vontades que não a sua própria.

De acordo com Peces-Barba Martinez (2003, p. 11), a luta pela afirmação da dignidade da pessoa humana como fonte dos direitos fundamentais do indivíduo é fortalecida por volta do século XX após a Segunda Guerra Mundial, em um movimento global que exigiu o respeito à condição humana como valor supremo de todos os sistemas jurídicos de inspiração democrática.

Fabio Konder Comparato (2010, p. 39), acrescenta que neste século teria sido atingida a última etapa da construção do conceito de dignidade da pessoa, juntamente como a filosofia do pensamento existencialista em que buscou acentuar o caráter único da personalidade

individual, possuindo cada ser uma identidade singular, inconfundível com a de outro qualquer. Por isso, ninguém pode experimentar a vida ou a morte de outrem, sendo realidades únicas e insubstituíveis.

Em um movimento de expansão, diversas Constituições germinadas neste período histórico passaram a expressar e reconhecer a dignidade da pessoa humana como um princípio fundamental dos Estados, tanto no âmbito interno da sua soberania quanto no âmbito internacional. Em destaque as Constituições do México, de 1917 e da Alemanha de Weimar, de 1919, assim como a da Finlândia no mesmo ano (1919), a de Portugal, em 1933, a da Irlanda, em 1937, a de Cuba, em 1940 e a da Espanha, em 1945.

Com o pós Segunda Guerra surge a Organização das Nações Unidas – ONU, em 1945 e consequentemente a Declaração Universal dos Direitos Humanos em 1948, que ratificou a dignidade da pessoa humana como um valor universal a ser almejado por toda a comunidade internacional, por se tratar da garantia dos valores mais fundamentais e essenciais à existência digna do indivíduo.

A partir da internacionalização da dignidade da pessoa humana e dos direitos humanos correlatos, o sistema constitucional brasileiro também fora influenciado por esse movimento de vanguarda que buscou a emancipação do indivíduo enquanto sujeito de direitos e senhor da sua própria existência, sobretudo após a promulgação da Constituição Federal de 1988, que surgiu como fruto de uma renovação político-social que resgatou a democracia no país após anos de ditadura militar.

Uma vez situado como princípio basilar da Constituição Federal de 1988, previsto no seu artigo 1º, inciso III, o legislador constituinte brasileiro erigiu à ideia de dignidade da pessoa humana a qualidade de norma embasadora de todo o sistema constitucional, orientando e irradiando sua aplicação a todo o ordenamento jurídico, tanto no que ao tange ao direito público quanto ao direito privado.

E neste mesmo sentido entende Jeremy Waldrom (2007, p. 203-204), quando evidenciou o que chamou de uma “dualidade de usos” para a acepção da dignidade humana, visto que opera tanto como a fonte dos direitos humanos e fundamentais, quanto também assumindo a condição de conteúdo dos direitos.

De certo, dentre as múltiplas possibilidades interpretativas de certo texto normativo, deve-se priorizar aquela concepção que assegure que o princípio constitucional da dignidade

da pessoa humana seja contemplado na maior amplitude possível e de forma eficaz, ao mesmo tempo em que este mesmo princípio atua como conteúdo valorativo das normas constitucionais e infraconstitucionais.

Nas lições de Ricardo Maurício Soares se pode apurar a extensão valorativa dada ao princípio da dignidade da pessoa humana:

> [...] o princípio ético-jurídico da dignidade da pessoa humana importa o reconhecimento e tutela de um espaço de integridade físico-moral a ser assegurado a todas as pessoas por sua existência ontológica no mundo, relacionando-se tanto com a manutenção das condições matérias de subsistência quanto com a preservação dos valores espirituais de um indivíduo que sente, pensa e interage com o universo circundante. (2010, p. 128).

E esta é a realidade inerente aos direitos da personalidade. Também embasada no princípio da dignidade da pessoa humana, a tutela da personalidade visa assegurar o desenvolvimento das características mais essenciais do indivíduo, resguardando a sua integridade física e psicológica para que se possa construir um sujeito que possua autonomia para gerir a própria existência.

Ao se proteger as esferas da intimidade e do segredo, buscou o legislador a contemplação do respeito à dignidade humana como um valor fundamental, criando mecanismos jurídicos para se evitar tal violação, a exemplo das ferramentas previstas no âmbito da responsabilidade civil.

E de igual forma, ao se concluir que a intimidade do indivíduo é também embasada na noção de dignidade humana, amplia-se também a tutela da privacidade ao meio digital, realidade do século XXI, devendo-se assegurar meios para se proteger a seara intocável do cidadão contra a curiosidade invasiva de terceiros e, porque não, do próprio Estado, de modo a resguardar a sua personalidade.

A omissão estatal neste sentido favorece a mitigação da privacidade e, consequentemente, da própria dignidade humana. Assim, de acordo com os ensinamentos de Ingo Sarlet (2012, p. 102), "sem que se reconheçam à pessoa humana os direitos fundamentais que lhe são inerentes, em verdade estar-se-á negando-lhe a própria dignidade".

Uma vez evidenciada a íntima correlação existente entre a dignidade da pessoa humana e a proteção dos direitos da personalidade, cabe-nos melhor esclarecer a origem da tutela da privacidade, de modo à melhor sedimentar o tema.

2.5 O SURGIMENTO DA PROTEÇÃO À PRIVACIDADE E INTIMIDADE

Podemos identificar na história bíblica de Adão e Eva um dos primeiros relatos onde se constata uma preocupação genuína com a privacidade. Os primeiros seres humanos do paraíso viviam em harmonia entre si e com o meio ambiente em que viviam, frise-se, completamente despidos.

A ingenuidade humana teria sido perdida após se alimentarem de um fruto proibido, mesmo diante das orientações expressas do Criador em sentido contrário. Como consequência, uma das primeiras medidas fora sentir a necessidade de proteger a nudez com folhas, na tentativa de assegurar a própria intimidade[1].

O avançar da história impõe aos homens muitos séculos de subjugação aos impérios, a exemplo do retrato da Idade Média, de modo que não se cogitava em qualquer tipo de garantia de proteção à vida, à saúde ou à integridade física de nenhum indivíduo, muito menos da privacidade.

Entretanto, já se podia evidenciar que a estratificação social típica do Estado Absolutista permitia que alguns poucos privilegiados pudessem isolar-se em seus castelos, manifestando algum resquício de privacidade, ainda que de cunho primitivo.

Já no contexto do Estado Feudal, alguns indivíduos, ainda que componente de uma casta inferior, poderiam esboçar algum sinal da privacidade quando optassem pela fuga da vida pública em prol da solidão, a exemplo dos eremitas, dos religiosos em seus mosteiros, ou ainda daqueles escolhidos para trabalhar para os senhores feudais.

Somente a partir do século XVI se pode constatar alguma mudança neste paradigma no que tange à privacidade em detrimento da vida em sociedade. Danilo Doneda (2006, p. 127) chama a atenção para o fato de que a evolução arquitetônica favorece a separação dos homens em classes e categorias e também ao isolamento, quando então começa a se delinear uma nova forma de se vislumbrar a privacidade do indivíduo em sociedade.

Contudo, antes do século XIX, a privacidade não era juridicamente tutelada diretamente por nenhum dos sistemas jurídicos mais significantes, seja o romano-germânico seja o anglo-saxão, haja vista que a sociedade rudimentar e de baixa complexidade não exigia

[1] BÍBLIA Sagrada: Antigo e Novo Testamento – Gênesis.

uma proteção normativa relevante no que tange à proteção da intimidade e da vida privada das pessoas.

Conforme Paulo José da Costa Júnior (1995, p. 13), há os que entendem que a proteção da vida privada teria sido judicializada pela primeira vez em território Francês, através do julgado do Tribunal Civil de Sena, em 16 de junho de 1858. A celeuma originou-se de um desenho confeccionado por dois artistas a pedido consciente de uma mulher no leito de morte. O desenho fora exposto à venda em um estabelecimento e o Tribunal determinou a sua apreensão, como uma medida que assegurava a privacidade da falecida.

Entretanto, a doutrina é pacífica ao constatar que fora em território norte-americano, em um artigo escrito por *Samuel Warren* e *Louis Brandeis*, intitulado *The right to privacy*, datado de 1890, onde se construiu a noção contemporânea de privacidade, desvencilhando-a da noção tradicional da propriedade até então retratada.

Este entendimento de vanguarda fora responsável por evidenciar a privacidade de forma autônoma sem uma ligação exclusiva com o direito à propriedade, mas sim, como requisito indispensável para a garantia da inviolabilidade da intimidade do indivíduo. O artigo retrata a denúncia dos autores contra a atuação de jornalistas sensacionalistas e contra o manejo arbitrário de aparatos tecnológicos como ferramentas para a invasão da privacidade das pessoas e exposição pública da sua intimidade. (WARREN; BRANDEIS, 1890, p. 195).

O pensamento exposto por Warren e Brandeis fora capaz de consolidar um ponto chave na construção histórica da privacidade, e consiste no reconhecimento da *inviolate personality*:

> *The principle which protects personal writings and other personal productions, not against theft and physical appropriation, but against publications in any form, is in reality not the principle of private property, but that of an inviolate personality*. (WARREN; BRANDEIS, 1890, p. 196).

Esta concepção originada nos Estados Unidos contribuiu para um aperfeiçoamento global do instituto, influenciando inclusive a Europa e algumas das mais importantes nações democráticas do Ocidente. Entretanto, durante o século XX, as transformações tecnológicas e a reestruturação da função do Estado proporcionaram mais uma modificação na concepção da privacidade.

No que tange à terminologia "privacidade", cabe tecer alguns esclarecimentos. Conforme Diógenes Ribeiro (2003, p. 21) a expressão derivaria do inglês '*privacy'*,

entretanto, na perspectiva de Danilo Doneda (2006, p. 107) o vocábulo teria raiz latina ‘*privare’*, cujo adjetivo seria ‘*privatus’*, embora reconheça que a expansão do uso tenha sido influenciada pelo emprego na língua inglesa, em uma expressão de anglicismo.

Já conforme Paulo José da Costa Júnior (1995, p. 25), a correta expressão seria ‘privatividade*’*, em um bom vernáculo, haja vista que se origina do termo ‘privativo*’*. Segundo o autor, o uso da expressão ‘privacidade’, seria fruto de um incorreto uso do português e, assim como Doneda (2006), bom exemplo de anglicismo.

De certo, independente da expressão a ser utilizada, não se pode deixar de pontuar que, diante da profusão de expressões similares utilizadas pela doutrina brasileira, tais como “privacidade” propriamente dita, “vida privada”, “intimidade”, “segredo”, “sigilo”, “recato”, “reserva”, “privatividade” (DONEDA, 2006, p. 101), dentre outros, o termo semântico mais adotado, e que também vem sendo referida neste trabalho é “privacidade”.

De acordo com José Afonso da Silva, deve-se entender o direito à privacidade “num sentido genérico e amplo, de modo a abarcar todas essas manifestações da esfera privada e da personalidade” (SILVA, 1996, p. 188), fazendo referência à garantia prevista na Constituição Federal de 1988, no seu art. 5º, inciso X.

É importante ainda ponderar que até mesmo o uso da expressão em inglês – *privacy* – exigiria cautela, considerando que “no ordenamento norte-americano, o *right to privacy* assume um caráter bastante abrangente, que deve ser devidamente filtrado para ser transposto para a nossa cultura jurídica”. (DONEDA, 2006, p. 137). Atualmente, constata-se que a *privacy* compreende noções muito mais complexas do que simplesmente o isolamento do indivíduo ou a tutela da sua tranquilidade. (DONEDA, 2006, p. 10).

Além da progressiva positivação deste direito no cenário internacional e também no âmbito da soberania interna dos Estados, os desafios contemporâneos de um mundo globalizado fizeram surgir a necessidade de atenção à proteção dos dados pessoais a partir da expansão dos bancos de dados informatizados.

2.6 A INTIMIDADE, O SEGREDO E A PROTEÇÃO AOS DADOS PESSOAIS

Diante da moderna sociedade da informação, gestada em decorrência do grande avanço tecnológico jamais experimentado em épocas anteriores, a vida privada do indivíduo

parece ter sido ameaçada, haja vista as inúmeras ferramentas de controle comportamental disponíveis no mercado de consumo, a exemplo das câmeras de vigilância e *webcams*, dos drones, dos *smartphones*, das mídias sociais, dentre outros.

Não restam dúvidas de que este momento histórico gera reflexos significativos sobre a intimidade das pessoas, haja vista que a sua exposição, mesmo não autorizada, ainda é objeto de interesse por parte da população. Todavia, a violação da esfera íntima e do segredo do indivíduo tem íntima correlação com o monitoramento do tráfego de dados pessoais na internet.

A intimidade pode ser conceituada como o "direito de impedir o acesso de terceiros aos domínios da confidencialidade". Integram o campo de tutela deste direito, como dito, as confidências, entretanto vão muito mais além, incluindo os informes de ordem pessoal ou os dados pessoais. (BITTAR, 2006, p. 111-112).

Podemos ainda acrescentar, as recordações pessoais, as memórias, os diários, as relações familiares, as lembranças de família, a sepultura, a vida amorosa ou conjugal, a saúde física ou mental, as afeições, os entretenimentos, os costumes domésticos e as atividades negociais. (BITTAR, 2006, p. 111-112). Não se trata de uma enumeração em *numerus clausus*, mas sim, em rol meramente exemplificativo.

Neste sentido, Paulo José da Costa Júnior (1995, p. 34) acrescenta que, integrando o direito à intimidade, seriam tutelados dois interesses consecutivos: o primeiro, no sentido de impedir que a intimidade não venha a ser objeto de violação e de curiosidade de terceiros; e, o segundo, no sentido de que o segredo e a intimidade não sejam divulgados indevidamente, o que potencializaria a transgressão e os danos.

De fato, diante de uma conjuntura moderna onde praticamente todo ato humano é realizado através dos recursos tecnológicos, desde o entretenimento às transações bancárias mais complexas, as informações e dados pessoais disponibilizados nestas oportunidades são objeto de armazenamento em grandes bancos de dados que, muitas vezes, estão sob a ingerência exclusiva das empresas privadas.

Em consequência, estes dados coletados estão vulneráveis à disponibilização e ao compartilhamento indevido a terceiros e ao monitoramento das rotinas comportamentais dos indivíduos, de modo estabelecer perfis de consumo estratégicos a cada segmento empresarial. Deste modo, a intimidade das pessoas vem sendo tratada como um produto do mercado de consumo e não mais como uma garantia fundamental inviolável.

Além da intimidade, a nova rotina tecnológica também vem evidenciando um cenário ameaçador no que tange à proteção do sigilo, a esfera última e inviolável do indivíduo. Carlos Alberto Bittar (2006, p. 124) nos esclarece que enquanto a tutela da intimidade cuida acerca de "aspectos mais amplos da esfera privada propriamente dita", o sigilo faz referência a fatos precisos e especificados, "conservados no âmago da consciência, por não convir ao interessado a sua divulgação, seja em virtude de razões personalíssimas (confidências), seja em razão de atividade profissional ou comercial."

Acrescenta o autor que existem elementos que poderiam identificar e particularizar o direito ao segredo, o que compreende "o sigilo pessoal; o sigilo documental; o sigilo profissional e o sigilo comercial". (BITTAR, 2006, p. 123). No mesmo sentido entende Costa Júnior (1995, p. 52).

Todos estes interesses integrantes da esfera última da privacidade se submetem às mesmas garantias contra a manipulação, armazenamento e compartilhamento indevido das informações obtidas através dos recursos tecnológicos modernos.

Não é demais acrescentar que a proteção do segredo é uma prerrogativa que também é inerente às pessoas jurídicas, haja vista que a estas também se aplica a tutela inerente aos direitos da personalidade, naquilo que for compatível, conforme determinação expressa no art. 52 do Código Civil Brasileiro, de 2002.

Desta forma, os dados pessoais das empresas também deve ser objeto de proteção legal, da mesma forma que às pessoas físicas, vedando-se a divulgação de informações restritas sobre o *know-how* de uma atividade empresarial, ou dados pessoais dos seus sócios, muito menos por meio da exploração comercial.

Diante da hipótese de violação da intimidade e do segredo dos indivíduos por meio da manipulação arbitrária dos seus dados pessoais obtidos por meio da internet, deve o ordenamento jurídico disponibilizar um rol de medidas de proteção a esses direitos, sobretudo nas ocasiões onde se constata a espionagem e a consequente revelação de dados pessoais e/ou confidenciais ou ainda no caso de indiscrições não justificadas.

De fato, não se pode perder de vista que o direito à intimidade nem sempre pode ser exercido em caráter absoluto, haja vista que em uma vida em sociedade, não raro, os interesses coletivos exigem prevalência sobre as vontades particulares, quando em prol do legítimo interesse público.

Muitas vezes em uma dada situação real da vida cotidiana, o direito à intimidade é posto em rota de colisão com outros direitos fundamentais, tal como o direito à informação. Nestes casos, conforme doutrina de Robert Alexy (2012, p. 93-99), deve-se realizar a ponderação dos interesses conflitantes quando, em determinada situação, um deles deverá receber a precedência em face do outro.

Em regra, a intimidade, o segredo e, consequentemente, os dados pessoais dos indivíduos não devem estar sujeitos à ingerência pública ou privada de terceiros, muito menos no meio digital, sob pena de violação do direito em causa, haja vista que expõe os atributos essenciais inerentes à pessoa humana e à sua dignidade.

De igual forma, é condenável, inclusive para fins comerciais, sem o consentimento do interessado, o compartilhamento dos dados pessoais eventualmente coletados e armazenados em virtude de alguma transação realizada por meio das ferramentas tecnológicas, a exemplo das fichas de bancos, dos cadastros em lojas de crédito ou entidades a que pertença o interessado, que somente as pode utilizar para a finalidade específica para a qual se obrigou: a abertura de contas; a concessão de crédito; a venda de bens. (BITTAR, 2006, p. 116).

Stefano Rodotá (2008, p. 17) chama a atenção para uma situação importante no que tange à tutela da intimidade e dos dados pessoais dos indivíduos. Segundo o autor, a tutela da vida privada e da intimidade consiste basicamente em impedir a interferência sob a vida pessoal e familiar de um indivíduo, manifestando-se como um tipo de "proteção estático" um "negativo".

Por outro lado, a proteção dos dados pessoais dos indivíduos "estabelece regras sobre os mecanismos de processamento de dados e estabelece a legitimidade para a tomada de medidas", manifestando, entretanto, como um tipo de "proteção dinâmico", ou seja, aquele que monitora o tráfego dos dados em todos os seus movimentos.

Importa, pois, em se assegurar juridicamente a possibilidade de manejo de instrumentos capazes de limitar a liberdade de atuação de terceiros no que tange à indiscrição sobre a vida alheia, e, de igual forma, se utilizar de ferramentas para obstacularizar que este mesmo terceiro o transmita a outrem o dado ou informação pessoal auferido por meio da intromissão indevida sobre a intimidade alheia, sobretudo no meio digital.

Cabe ainda ressaltar que, por via de regra, com a morte se extingue a possibilidade de lesão à intimidade do indivíduo, situação esta retratada através do brocardo latino *mors omnia solvit*. Entretanto, o melhor entendimento é aquele que reflete que, ao contrário, alguns dos

direitos da personalidade devem permanecer íntegros após o falecimento, tais como a intimida e o segredo do *de cujus*.

Isto porque tais atributos da personalidade podem sim ser violados no *post mortem*, pois, a esfera íntima do falecido pode vir a ser violada com a divulgação posterior dos seus segredos e intimidades, seja legítima ou ilegitimamente adquirido. (COSTA JÚNIOR, 1995, p. 58). Esta seria também, por exemplo, a hipótese de terceiros que se apropriam de dados pessoais dos falecidos, a exemplo do nome, CPF ou ainda um perfil nas mídias sociais para auferir vantagens ou divulgar fatos que violem a imagem ou a honra do outrora titular.

A tutela da privacidade vem demonstrando novas configurações na sociedade moderna, pautada no avanço tecnológico e na rápida divulgação das informações, sobretudo diante da rede mundial de computadores. Esta realidade retrata que a sociedade vem evoluindo historicamente e socialmente, merecendo o acompanhamento da respectiva proteção jurídica frente às novas ameaças aos direitos fundamentais.

3 OS DADOS PESSOAIS E A SOCIEDADE DE CONSUMO

3.1 A SOCIEDADE DA INFORMAÇÃO E DO CONSUMO

O século XXI é marcado pelo avanço tecnológico e pela relativização das barreiras territoriais das nações. O processo da globalização permitiu uma maior integração entre os povos, sobretudo após o surgimento do computador e da internet. A informação nunca se difundiu de forma mais rápida, e um acontecimento ocorrido em uma parte do globo logo chega ao conhecimento dos demais indivíduos.

É o momento do surgimento de uma sociedade da informação, caracterizada pela criação de ferramentas que favoreceram a difusão do conhecimento e da comunicação entre os povos, aproximando línguas, culturas e tradições. Entretanto, cabe mencionar que esta sociedade é dinâmica e complexa, manifestando sempre o potencial de expansão e readaptação com os valores cultuados pela comunidade.

Conforme Jean Baudrillard, a vida cotidiana é o local do consumo. Para o autor, na contemporaneidade, o consumo aponta para a felicidade justamente por um defeito no que tange à resolução das tensões sociais. (BAUDRILLARD, 2007, p. 16-17).

Neste sentido, a sociedade do consumo não se caracterizaria apenas e tão somente pelo aumento dos gastos individuais, mas também pelo crescimento dos gastos assumidos por terceiros, sobretudo pelo Estado, de modo a reduzir as desigualdades sociais na distribuição dos recursos. (BAUDRILLARD, 2007, p. 19).

E com esta mesma sociedade que fomenta a interação entre os indivíduos e o acesso rápido às informações sobre o que ocorre a cada momento no planeta, surgem novos desafios à promoção dos direitos fundamentais, sobretudo no que tange à proteção da privacidade e da intimidade. Não é outro o entendimento de Bauman, ao afirmar que na "sociedade de consumidores, a dualidade sujeito-objeto tende a ser incluída sob a dualidade consumidor-mercadoria". (BAUMAN, 2008, p. 30).

A internet modificou completamente a rotina das sociedades, sobretudo pela possibilidade de acessá-la a qualquer hora e em qualquer lugar, criando uma esfera virtual que não pode ser ignorada. (EFING, 2002, p. 187). Hoje o trabalho pode ser executado na própria

casa do empregado, por meio do *Home Office*, utilizando a tecnologia como ferramenta para a redução dos custos empresariais.

As lojas virtuais ampliam cada vez mais a fatia de mercado e o espaço que antes era destinado às lojas físicas. A liberdade de escolha do consumidor aliado ao preço competitivo oriundo dos menores custos de operação do empresário são fatores preponderantes para que o *e-comerce* expanda seu campo de atuação na sociedade da informação.

Esta conjuntura deveria servir para o aprimoramento da vida social e das relações humanas, visando atuar como instrumento da integralização da satisfação dos indivíduos, bem como o manejo da tecnologia a serviço do homem. (MANSO, 1995, p. 20). Entretanto, os interesses de mercado acabam prevalecendo.

A sociedade da informação ainda proporcionou um efeito colateral não previsto: até mesmo os ilícitos penais necessitaram se adaptar à realidade, surgindo novos tipos penais para regular as condutas típicas que, agora, podem ser cometidas à distância, a exemplo daquelas disciplinadas na Lei nº 12.737/2012, também conhecida como a "Lei dos Crimes Cibernéticos".

Inúmeras são as ameaças à privacidade que a sociedade da informação nos apresenta, a exemplo das câmeras de vigilância em locais públicos e privados, da exposição indevida de informações pessoais nos meios de comunicação, da violação do sigilo sobre o acesso na rede mundial de computadores, da interceptação cada vez mais frequente de dados e registros telefônicos ou, ainda, do armazenamento indevido de dados pessoais dos cidadãos em bancos de dados informatizados e de ampla capacidade.

Como bem referido por Têmis Limberger (2007, p. 51), atualmente todos os computadores estão conectados em rede, e não mais isolados. Isso traz um efeito importante na sociedade atual que é o fato de que as informações veiculadas transportam-se do âmbito restrito do lar à transmissão global em velocidade excepcional, entrelaçando fatores como espaço e tempo.

E no mesmo sentido é o entendimento de Paulo José da Costa Júnior (1995, p. 28) quando constata ser inegável que novos problemas com a era da tecnologia vêm causando grandes repercussões no plano jurídico, sobretudo através da cibernética, que vem gerando um novo sistema de interação entre o homem e a máquina. Diante dessa realidade, é fundamental uma análise cuidadosa sobre como disciplinar estas relações.

E acrescenta o autor:

> O processo de corrosão das fronteiras da intimidade, o devassamento da vida privada, tornou-se mais agudo e inquietante com o advento da era tecnológica. As conquistas desta era destinar-se-iam em tese a enriquecer a personalidade, ampliando-lhe a capacidade de domínio sobre a natureza, aprofundando o conhecimento, multiplicando e disseminando a riqueza, revelando e promovendo novos rumos de acesso ao conforto. (COSTA JÚNIOR, 1995, p. 22).

Esta Era da Informação parece exigir uma reformulação nas "tábuas de valores" (RODOTÀ, 2008, p. 58) da sociedade, e isto no sentido de assegurar a plena expansão da liberdade e da democracia. O avanço tecnológico e globalizatório nos deparam com uma realidade que, da mesma forma que amplia conhecimentos, ameaça a existência de muitos dos direitos fundamentais, e entre eles está incluído o direito à privacidade.

De acordo com Anthony Giddens, a expansão da globalização não pode ser considerada apenas como uma realidade inerente aos grandes sistemas, mas sim que a "globalização não é apenas uma coisa que <<anda por aí>>, remota afastada do indivíduo. É também um fenômeno <<interior>>, que influencia aspectos íntimos e pessoas das nossas vidas". (GIDDENS, 2000, p. 23).

Como então explicar este caráter ambivalente da sociedade da informação? Uma resposta coerente poderia estar no fato de que, historicamente, a maioria das grandes descobertas científicas e tecnológicas que poderiam beneficiar milhões de pessoas, foram corrompidas ao serem convertidas em produtos de consumo. A partir do momento em que a segurança tornou-se um mercado de consumo, a privacidade manteve-se em risco.

Entre os meios de comunicação de mídia, a privacidade e a intimidade das pessoas passou a ser vista como uma fonte de renda, sobretudo quando o foco são as pessoas públicas, através da veiculação de notícias e fotografias em revistas e programas sensacionalistas. Ocorre que através de uma regra básica da economia, só há oferta quando há demanda. Este tipo de produto é consumido por grande parte da sociedade, de modo a refletir os valores sociais cultivados atualmente. E esta é uma das consequências da sociedade da informação e do consumo.

Segundo Costa Júnior (1995, p. 25-26),

> não podemos permanecer indiferentes quando os meios de comunicação de massa realizam um tipo de expropriação da vida privada por "curiosidade pública", quando a tecnologia põe ao alcance de indiscretos e bisbilhoteiros instrumentos verdadeiramente diabólicos, para penetrarem em nosso "jardim secreto" e transformarem nossa solidão em ingênua aparência."

Hodiernamente, diante da enorme capacidade de armazenamento e processamento de dados pessoais por meio de empresas que realizam uma detalhada análise de perfil das pessoas a fim de efetuar uma condução estratégia do seu negócio, a vigilância tornou-se mais frequente. O resultado é a “classificação das pessoas em categorias de acordo com a avaliação de seus riscos e a discriminação do acesso a determinados bens e serviços.” (MENDES, 2014, p. 91).

Se por um lado se evidencia um grande lucro à empresa diante da estratégia de análise de perfil, que muitas vezes ainda é terceirizado, e que termina por reduzir os custos e a concorrência, por outro lado, se potencializa uma grande ameaça à personalidade do consumidor, acaso de adote a estratégia de se utilizar do fluxo de dados pessoais para limitar indevidamente o acesso dos consumidores e bens e serviços ou classificá-los de forma discriminatória. (MENDES, 2014, p. 91).

Uma vez evidenciados alguns reflexos inerentes ao surgimento da Sociedade da Informação e consequentemente da Sociedade do Consumo e seus reflexos sobre o direito à privacidade, cabe um maior aprofundamento sobre a tutela da intimidade e dos dados pessoais.

3.2 A INFORMAÇÃO NA ERA DA INTERNET

Uma forma eficaz de se regular o progresso experimentado pela sociedade está na sua capacidade de armazenar e transmitir as informações, quando então as questões que envolvem espaço e tempo têm seu alcance reduzido. Contribuindo diretamente neste cenário está o surgimento da internet e a ampliação gradual da sua acessibilidade a todos os povos do planeta.

O indivíduo assume a sua personalidade perante um novo espaço social: o digital. Trata-se de uma arena onde as pessoas assumem perfis que geram um imenso fluxo de informações e dados através do acesso a sítios na rede e troca de mensagens entre usuários em uma rede aberta onde muitos podem ter acesso a ela.

Os dados pessoais gerados com a navegação na internet são armazenados e geridos pelo Estado e por empresas privadas, que os mantém em grandes bancos de dados que se

mostram capazes de cruzar as informações para evidenciar os padrões de comportamento dos indivíduos, o que tornará possível traçar perfis para tomada futura de decisões.

E a tecnologia atual de processamento de dados é capaz de facilitar a manipulação destas informações. Para o Estado, os dados individuais coletados e armazenados podem se mostrar importantes para traçar perfis acerca das necessidades públicas em cada localidade, favorecendo a implementação de políticas públicas eficazes e com menor desperdício de recursos públicos.

Entretanto, estes mesmos dados, se mal utilizados, podem oferecer informações detalhadas sobre a vida dos cidadãos, atuando como uma ferramenta para o controle sobre seus comportamentos, violando as prerrogativas da liberdade e do regime democrático.

No que tange às empresas privadas, a capacidade de armazenamento de dados em grandes bancos de dados tem o condão de possibilitar o cruzamento destas informações para se estabelecer padrões e perfis de consumo, de modo a impulsionar o lucro do mercado com estratégias quase sempre realizadas à revelia do titular dos dados.

De igual forma, para além de uma mera tentativa de ampliação do lucro, os dados pessoais armazenados sem qualquer controle sob a posse de empresas privadas podem ainda serem utilizados como uma ferramenta oculta para se negar o acesso de alguns consumidores aos bens e serviços por conta de uma análise de perfil que, muitas vezes, fora obtido por meios que violaram a intimidade do indivíduo.

Neste sentido, chama a atenção Danilo Doneda (2006, p. 2)

> Nossos dados, estruturados de forma a significarem para determinado sujeito uma nossa representação virtual ou um *avatar*, podem ser examinados no julgamento de uma concessão de uma linha de crédito, de um plano de saúde, na obtenção de um emprego, na passagem livre pela alfândega de um país, além de tantas outras hipóteses.

Os dados pessoais refletem aspectos inerentes aos direitos da personalidade e, como tal, merecem a devida proteção pelo ordenamento jurídico. Para tanto, deve-se delinear esforços para a proteção da liberdade negativa do indivíduo, no sentido de se impedir que a sua seara íntima possa ser devassada pela curiosidade alheia, seja pelo próprio Estado e seja pelos particulares.

Hodiernamente, considerando a forma como vem sendo realizado o processamento em massa das informações, não se deve pensar a tutela da privacidade da mesma forma que se

manifestou para outras sociedades. A realidade tecnológica com a qual convivemos nos depara com novas hipóteses de tutela e novas ameaças aos direitos fundamentais.

Diante da sociedade da informação, com a qual convivemos, "nós somos as nossas informações", haja vista que elas "nos definem, nos classificam, nos etiquetam" e, desta forma, ter o controle sobre as informações pessoais, sobre a forma como se dissemina e saber quem as usa significa adquirir, de forma concreta, o poder sobre sua própria existência. (RODOTÁ, 2008, p. 7).

Um dos problemas centrais evidenciados quando nos deparamos com a forma como se processam os dados pessoais na internet é que, diante da intensidade do fluxo dos dados pessoais, muitas vezes torna-se árdua a tarefa de se ter o conhecimento de quem efetivamente os detém e da forma como eles serão utilizados, tornando a tarefa de controle destas informações um grande desafio.

Diante desta realidade, torna-se cada vez mais complicado se delimitar quais são os tipos de informações que, efetivamente, o indivíduo estaria disposto a renunciar no que tange ao controle sobre estes dados e sobre as atividades mediante as quais os terceiros as utilizam. Isso nos chama a atenção para o fato de que mesmo as informações aparentemente mais irrelevantes podem, quando cruzadas com mais dados, proporcionar dados ao titular. (RODOTÀ, 2008, p. 36).

Por outro lado, acrescenta Stefano Rodotá que

> [...] a nova situação determinada pelo uso de computadores no tratamento das informações pessoais torna cada vez mais difícil considerar o cidadão como um simples "fornecedor de dados", sem que a ele caiba algum poder de controle. [...] As informações coletadas não somente tornam as organizações públicas e privadas capazes de planejar e executar os seus programas, mas permitem o surgimento de novas concentrações de poder ou o fortalecimento de poderes já existentes. (2008, p. 36-37).

Entretanto, mesmo diante da constatação acerca do caráter invasivo das atuais tecnologias da informação, que se apoderam das transações comerciais, das relações sociais ou das atividades políticas, ao mesmo tempo, não mais podemos nos entregar à completa "renúncia tecnológica", abdicando das benesses que a evolução nos proporciona.

3.2.1 Uma necessária precisão de conceitos: Dados vs Informação

Conforme Raymond Wacks (1989, p. 25), o "dado" pode ser definido como uma informação em potencial, haja vista que, quando coletada, tratada e assimilada, pode vir a se transformar em uma informação útil. Em sendo o caso de dados manifestados sob a forma de sinais que exijam prévia correlação e interpretação, é considerado como uma "pré-informação", até que possa ser decodificado por alguém habilitado.

Neste sentido, nem todo dado consubstanciaria em uma informação, embora toda informação seja oriunda da coleta de dados sobre determinado fato ou pessoa. Todavia, o estágio atual da expansão tecnológica já possibilita que grandes bancos de dados conectados em rede e com alta capacidade de processamento, possam cruzar estes dados sumariamente irrelevantes a fim de se extrair valiosas informações sobre o indivíduo.

Já de acordo com Têmis Limberger (2007, p. 61), o "dado pessoal é uma informação que permite identificar uma pessoa de maneira direta." Os dados de cunho pessoal conteriam informações privadas dos indivíduos que possibilitariam a sua identificação e reconhecimento, seja no momento atual ou posteriormente.

De acordo com a experiência europeia, a definição de "dados" constante do artigo 2º da Diretiva 95/46/CE pode ser auferida do fato de que se refere a

> qualquer informação relativa a uma pessoa singular identificada ou identificável ("pessoa em causa"); é considerado identificável todo aquele que possa ser identificado, directa ou indirectamente, 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. (COMUNIDADE EUROPEIA, 1995).

Nem todos os dados inerentes a um determinado indivíduo são relevantes o suficiente para merecer a tutela jurídica contra aquele que os divulga. Existem outros dados, os pessoais, que, entretanto, são mais específicos e retratam situações da vida privada e da intimidade dos indivíduos, e que são juridicamente tutelados pelo fato de serem inerentes à dignidade da pessoa humana e materializarem características fundamentais da personalidade.

No que se refere à dicotomia entre expressões como "informação" e "dados", cabe evidenciar que ambos os conteúdos podem se sobrepor em circunstâncias variadas, "o que justifica uma certa promiscuidade na sua utilização". (DONEDA, 2006, p. 152).

Acrescenta Danilo Doneda que

> o “dado” apresenta conotação um pouco mais primitiva e fragmentada, [...] o dado estaria associado a uma espécie de “pré-informação”, anterior à interpretação e ao processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição, e mesmo nos efeitos que esta pode apresentar para o seu receptor. [...] na informação já se pressupõe uma fase inicial de depuração de seu conteúdo – daí que a informação carrega em si também um sentido instrumental, no sentido de uma redução de um estado de incerteza. (2006, p. 152).

Uma definição para o termo “informação” fora descrita na Convenção de Strasbourg do Conselho Europeu, em 1981, segundo a qual, seria “qualquer informação relativa a um indivíduo identificado ou identificável”. Não restam dúvidas de que uma das características mais importantes é o fato da informação estar vinculada a uma pessoa, evidenciando alguma perspectiva da vida privada.

Não é demais esclarecer que um dado pode referir-se a uma pessoa indeterminada, como é o caso do dado anônimo. Esta ocultação dos dados com a consequente exclusão do vínculo existente entre a pessoa e a informação, é uma das ferramentas adotadas por leis modernas de proteção aos dados pessoais.

Entretanto, não podemos deixar de pontuar que o direito à privacidade não pode ser considerado como um direito absoluto, haja vista que o interesse coletivo legítimo permite alguma flexibilização na garantia deste direito. Neste sentido, não se pode perder de vista que a coleta e tratamento das informações nem sempre se mostra lesiva aos interesses do indivíduo.

Para que o Estado possa atingir a eficiência esperada na implementação de uma política pública necessita estar municiado de informação, sobretudo a de cunho censitário, de modo a estudar a melhor viabilidade na execução da função pública.

Contudo, o acúmulo de um grande número de informações nos bancos de dados do poder público possibilita o seu manejo como ferramenta de controle social e de manipulação dos cidadãos, estratégia esta que reflete uma das diretrizes inerentes aos regimes totalitários.

Ocorre que os grandes conglomerados transnacionais passaram a competir com o Estado no que tange ao controle dos dados, inaugurando imensos bancos de dados globais que pudessem melhor canalizar as estratégias de mercado. Com isso a privacidade também passa a ser relativizada diante dos grandes interesses econômicos.

Importante se esclarecer que a informação pessoal pode, de alguma forma, se dissociar do indivíduo, tornando-se exterior a ele e, neste sentido, circular pela rede mundial, ser

coletada, armazenada e manipulada. Contudo, em sendo considerada uma informação pessoal, permanece com a qualidade de identificação de um indivíduo, e tal informação deve ser entendida como uma extensão da personalidade. (DONEDA, 2006, p. 168).

3.3 A COLETA DOS DADOS PESSOAIS E O TRÁFEGO DE REGISTRO DE INFORMAÇÕES

Na sociedade atual, todo ato humano é capaz de gerar dados, seja pelo uso do celular, pelo envio de e-mails, por meio de transações bancárias ou através de compras no cartão de débito ou crédito. Estes dados podem conter os mais variados conteúdos, e, entre eles, está o dado pessoal, aquele que adentra a vida privada do indivíduo e que caracteriza a sua personalidade.

Estas informações colhidas muitas vezes à revelia do seu titular possibilitam o uso secundário com finalidade lucrativa, beneficiando os gestores destes sistemas. Os dados colhidos quando do fornecimento do serviço podem ser cruzados e transformados em informações que estabelecem perfis, geralmente de consumo, que interessam a terceiros que as adquirem.

Diante de possibilidades tão amplas de coleta dos dados disponíveis no mercado do consumo, não se pode permitir que o Direito esteja à margem desta realidade, omitindo-se quanto às consequências da violação da privacidade sobre os indivíduos. Estendendo esta tutela até a esfera virtual, é necessário se garantir ferramentas seguras de navegação na internet, valendo-se, por exemplo, da criptografia. (RODOTÁ, 2008, p. 155).

Stefano Rodotá (2008, p. 155) nos indica outra opção para se combater as medidas arbitrárias de coleta dos dados pessoais. Tratam-se das "*privacy enhancing technologies"* (PET), sítio certificados que disponibilizam um ambiente onde o usuário pode-se sentir mais seguro, sem que tenha seus rastros perseguidos por outros frequentadores da rede mundial.

A coleta dos dados privados dos indivíduos constitui uma fase muito importante no tratamento das informações. Antes do advento do computador e da consequente capacidade de processamento de dados, mostrava-se muito mais difícil ao comércio ter acesso às preferências, padrões e hábitos dos consumidores sem que houvesse o contato pessoal entre este e o vendedor.

Atualmente, todavia, as ferramentas tecnológicas permitiram que os dados pessoais fossem transmitidos em alta capacidade e frequência entre os interessados, agindo em verdadeiro monitoramento da vida cotidiana dos indivíduos, muitas vezes sem que o próprio consumidor tenha prévia ciência ou manifeste qualquer concordância inequívoca.

Neste sentido, torna-se necessária uma análise acerca de algumas das ferramentas utilizadas pelo Estado e por particulares no sentido de obter o êxito na coleta e tratamentos dos dados pessoais dos consumidores, seja revertendo estas informações em políticas públicas em prol da coletividade, seja em benefício das estratégias mercadológicas.

3.3.1 As Transações Comerciais

Trata-se da forma tradicional de coleta de dados pessoais por excelência. Nesta situação, o consumidor autoriza ao fornecedor de produtos e serviços, de forma voluntariamente e consentida, que o mesmo colete e armazene seus dados pessoais básicos a fim de manter um cadastro dos seus consumidores.

Em regra, a coleta e o armazenamento dos dados pessoais ocorrem com maior frequência na hipótese de compras a crédito. Muitas vezes, os formulários contemplam também registros de hábitos de consumo, de modo a possibilitar a oferta de produtos adequados.

Os cartões fidelidade também constituem ferramentas de coleta de informações no momento da compra. Com este tipo de estratégia o fornecedor de produtos e serviços pode monitorar a frequência de compras, quais as lojas mais frequentadas, em que dia o consumidor prefere fazê-las, se eles possuem filhos ou, ainda, quais são suas marcas e produtos favoritos. (MENDES, 2014, p. 96-97).

Entretanto, nesta técnica também pode ser evidenciado um grande potencial de violação à privacidade das pessoas. Um ponto fundamental é que, para que haja a coleta e o armazenamento dos dados, torna-se imprescindível a concordância do consumidor. Ademais, esta aceitação não pode ser viciada, como aquela auferida a partir de uma abordagem constrangedora ou coativa do fornecedor.

Neste sentido, ainda que o armazenamento dos dados pessoais tenha sido autorizado de forma sumária pelo cliente no momento da transação comercial, não há garantias de que as informações coletadas permanecerão exclusivamente sob a posse e guarda do fornecedor de

produtos e serviços, ou ainda, se as mesmas serão efetivamente utilizadas com a finalidade para que foram coletadas.

Por isso torna-se de extrema relevância a proteção da personalidade do indivíduo por meio de normas jurídicas que possam estabelecer as responsabilidades das empresas e dos consumidores no que tange à coleta dos dados pessoais, assegurando mecanismos para que aquele que os coletou não possa repassá-los a terceiros, seja de forma gratuita ou não.

3.3.2 O Recenseamento Demográfico

Para que o Estado possa gerir adequadamente os recursos públicos escassos, empregando-os de forma eficaz e igualitária entre às áreas necessitadas do seu território torna-se necessário ter o conhecimento prévio da quantidade de indivíduos residentes no país, algo que somente pode ser realizado através de recenseamento demográfico, de modo a possibilitar a implementação de políticas públicas eficientes.

Baseado em questionários pré-elaborados cujas perguntas e respostas são registradas em aparelhos portáteis, os analistas censitários do governo deslocam-se sazonalmente pelos municípios do país, coletando e registrando um grande volume de informações dos cidadãos, tais como a idade, a faixa de renda, a raça e a localização geográfica, refletindo um grande arquivo de dados pessoais.

Contudo, em que pese à presunção de que o Estado sempre atua em benefício da coletividade, não se pode constatar de forem cabal o motivo pelo qual estes dados estão sendo coletados, qual a destinação a ser dada a eles, ou ainda, se os mesmos não estão sendo disponibilizados a terceiros.

Não se pode perder de vista que os dados coletados por meios dos censos públicos tanto podem se transformar em informação útil para a tomada de decisões em prol dos direitos e das garantias fundamentais, como podem, sob interesses escusos, serem compartilhados com empresas privadas a fim de potencializar o lucro, pouco importando com a violação da privacidade dos cidadãos.

Conforme evidencia Laura Schertel Mendes,

> é bastante questionável que os dados pessoais que foram coletados com o propósito de servir ao censo demográfico possam ser utilizados para fins de *marketing* direto ou avaliação de risco, sem o consentimento do titular, uma vez que isso viola o princípio da finalidade da proteção de dados pessoais. (MENDES, 2014, p. 98-99).

Desta forma, a construção de um marco legal no Brasil, no que tange à proteção dos dados pessoais, deve direcionar esforços à proteção da privacidade dos indivíduos, tanto em face da atuação arbitrária das empresas privadas, quanto diante da eventual postura tirana do próprio Estado.

3.3.3 As Pesquisas de Mercado

Mesmo diante das inúmeras potencialidades que um negócio possa desenvolver, todo um planejamento empresarial pode estar fadado ao fracasso se não houver informação, em grande número e variedade. De modo a se alimentar desta fonte, as empresas muitas vezes se valem das pesquisas de mercado como uma ferramenta de coleta de dados dos consumidores.

As pesquisas podem ser realizadas entrevistando-se o consumidor por meio das mais variadas ferramentas tecnológicas, sejam pessoalmente, por telefone, e-mail ou qualquer outra técnica que viabilize a interação. É de suma importância na vida cotidiana de uma empresa, possibilitando "conhecer o que os consumidores desejam e quanto estão dispostos a pagar, buscando obter uma vantagem competitiva". (MENDES, 2014, p. 99).

Em havendo o consentimento expresso do consumidor e destinando-se estritamente ao objetivo à qual fora realizada, não se pode identificar qualquer reprimenda a esta prática. Entretanto, sem a existência de um diploma legal que possa estabelecer regras e responsabilidades a todos aqueles que manipulam dados pessoais dos indivíduos, a vida privada sempre poderá estar ameaçada.

3.3.4 Os Sorteios

Não menos importante do que nenhuma das ferramentas anteriores, os sorteios e os concursos são técnicas eficazes na coleta de dados pessoais. Em muitas oportunidades, o preenchimento de questionários que estão associados aos sorteios é a única finalidade pela qual este se realizou, ainda quando esta estratégia passe despercebida aos olhos da maioria dos consumidores. (MENDES, 2014, p. 100).

Neste sentido, demonstra ser uma medida ilegítima quando utilizada exclusivamente com a finalidade de coletar dados, haja vista que viola a prerrogativa do consumidor de ter a ciência prévia do destino das informações a que lhe diga respeito, bem como se mostra arbitrária por não possuir o consentimento expresso do titular.

3.3.5 Cookies

No ambiente virtual da internet, as possibilidades de atentado à vida privada e à intimidade dos indivíduos são reais e não merecem ser desprezadas, sobretudo no que tange à coleta dos dados pessoais dos usuários, muitas vezes de forma capciosa e sem o consentimento expresso do titular. E uma das possibilidades surge com os *cookies*.

De acordo com Arnaud Belleil (2002, p. 65), os *cookies* são "pequenos ficheiros depositados no computador do internauta pelos sítios visitados", que adquirem acesso às aos dados e informações pessoais dos indivíduos, quase sempre atuando de forma oculta à identificação do usuário comum. Instalam-se no disco rígido dos computadores e auxiliam uma forma mais atual de *marketing*¸ aquela focada na "memorização e a análise dos movimentos efetuados" pelo internauta.

São utilizados como ferramenta oculta de coleta de informações, prevalecendo abusivamente da ignorância do usuário, que quase sempre desconhece que a cada sítio acessado gera uma trilha sobre seus hábitos, gostos e preferência, que são coletados por empresas privadas sem a sua expressa autorização e com finalidades duvidosas.

Não é demais evidenciar os limites desta ferramenta, através das palavras de Arnaud Belleil (2002, p. 67):

> Os *cookies* seguem um rastro e não um utilizador. Só podem tornar-se verdadeiramente ameaçadores se a máquina for associada a um utilizador. É o que acontece quando este forneceu, ao preencher questionários, por exemplo, o meio de estabelecer a ligação entre a sua identidade real e a navegação que está a efetuar a partir da sua máquina.

Ocorre que os *coookies* nem sempre podem ser entendidos, em toda e qualquer circunstância, necessariamente como invasivos. Por se tratarem de pequenos fragmentos de código inseridos nos computadores (JENNINGS;FENA, 2000, p. 65), eles são responsáveis, por exemplo, pelo acesso rápido aos programas de meteorologia, às caixas de entrada dos e-mails e aos sítios preferidos do usuário visitados recentemente, considerando que possibilitam o acesso a esses ficheiros já depositados no HD de modo a acelerar o desempenho.

As discussões envolvendo a possível ilegitimidade na utilização dos *cookies* já vêm sendo objeto de debates pelo mundo. Ao teor da Diretiva 2009/136/EG que alterou a Diretiva 2002/58/EG, no que tange à tutela da privacidade diante das comunicações eletrônicas, restou

consignado a exigência do prévio consentimento do consumidor para qualquer tipo de coleta de dados e informações armazenados nos computados, e aplica-se também aos *cookies*. (MENDES, 2014, p. 103).

O ordenamento jurídico brasileiro precisa acompanhar os avanços tecnológicos e sociais, se debruçando sobre os aprendizados que podem ser auferidos do Direito Comparado, de modo a melhor tutelar os interesses dos cidadãos e às garantias fundamentais previstas no texto constitucional.

3.3.6 *Spywares*

Podendo ser considerada uma "tecnologia de vigilância" (MENDES, 2014, p. 104-105) tanto quanto de coleta de dados, os *spywares* possibilitam a interceptação de mensagens, e o monitoramento das atividades desempenhadas pelo usuário no computador. São *softwares* espiões que são baixados diante de um acesso à internet, sem que o usuário comum tenha conhecimento da sua invasão ou manifeste qualquer consentimento neste sentido.

Certamente é questionável a legitimidade da utilização dos *spywares*, contudo, muitas vezes não é possível identificar a origem da invasão. O ataque pode partir desde agências de espionagem governamentais, passando por grandes empresas privadas, e chegando até jovens entediados e mal intencionados que dominam completamente a tecnologia, como os *hackers.*

Estes programas possibilitam o acesso às comunicações do usuário, como os e-mails pessoais, tomando conhecimento de toda a vida atual e pretérita do mesmo, bem como tudo aquilo que estiver armazenado do HD do computador, como registros de dados e imagens, fotos e vídeos de cunho privado. O usuário não consegue garantir a sua privacidade mesmo dentro da sua casa.

Por mais que haja um esforço exaustivo dos fornecedores de antivírus em combate este intruso indesejado, os *spywares* se expandem pela rede e geralmente são carregados "dissimulados em programas gratuitos que os internautas são convidados a telecarregarem no seu computador". (BELLEIL, 2002, p. 68).

Na internet, inúmeros são os interesses que podem manipular ferramentas ilegítimas de coleta de dados pessoais, como os *spywares*. Nesta rede, o usuário certamente é objeto de uma verdadeira devassa na sua privacidade, por via de regra, em prol dos interesses do mercado, exigindo que o ordenamento jurídico de cada nação acompanhe esta realidade.

3.3.7 *Spamming*

Os *spammings* são o exemplo de mais uma ferramenta cibernética utilizada para a coleta dos dados pessoais dos indivíduos, atuando como mais uma verdadeira ameaça à privacidade. São aquelas gamas de e-mails não solicitados que sobrecarregam as caixas de mensagem dos usuários com informações de cunho sexual, comercial ou até mesmo preconceituoso.

É uma ferramenta irritante a muito dos usuários e também nociva por atuar como porta de entrada para *sofwares* nocivos aos computadores e à privacidade dos navegantes. Se em um determinado dia o usuário pretenda consultar um determinado produto ou serviço para compra na internet, certamente muito em breve receberá inúmeras mensagens de e-mail com ofertas semelhantes. É mais um exemplo da privacidade sendo devassada.

A gravidade desta situação não passou despercebida nem mesmo à paciência de Bill Gates, quando reconheceu publicamente a grande dificuldade que é ser excluído da lista de um *spammer*. Para tanto, as alternativas de solução partem também da própria internet, através da difusão das *privacy enhancing technologies*, identificados como *softwares* capazes de realiar um filtro e excluir automaticamente as "mensagens-lixo". (RODOTÀ, 2008, p. 155).

Uma vez evidenciada algumas das estratégias utilizadas atualmente para a coleta dos dados pessoais dos indivíduos, tanto fisicamente quanto através da internet, torna-se oportuna uma análise acerca do destino destes dados coletados e o tratamento a que são submetidos.

3.4 A TECNOLOGIA E O TRATAMENTO DOS DADOS PESSOAIS DOS CONSUMIDORES

Além da ampla capacidade de coleta e de armazenamento dos dados pessoais materializados nos grandes bancos de processamentos de dados, a privacidade no que tange aos dados pessoais ainda pode estar sob ameaça de violação por meio de outras estratégias tecnológicas manejadas com o uso da internet, sobretudo pelas empresas privadas.

As maiores demandas que integram os casos de violação da privacidade atualmente são aquelas correlacionadas com a divulgação da informação e condicionadas pelo manejo da

tecnologia. A divulgação indevida dos dados pessoais é uma das causas mais relevantes da ocorrência da exposição não desejada de um indivíduo frente à sociedade.

Ocorre que a internet vem sendo estruturada e gradativamente associada exclusivamente a um espaço voltado ao comércio, reduzindo a tutela dos direitos e garantias fundamentais apenas no que tange àqueles ligados à troca de bens e serviços. É preciso combater esta realidade que reduz o papel do cidadão ao de um consumidor, impedindo-se que a "esfera pública e a privada sejam absorvidas na esfera da produção e da troca". (RODOTÀ, 2008, p. 157-158).

Consoante a este sentido nos acrescenta Arnaud Belleil (2002, p. 18-19)

> A Internet traz a doença: a concorrência. A Internet proporciona a solução: a personalização. E se o remédio induzisse um efeito secundário ainda mais nefasto do que a própria doença? O efeito secundário é a destruição da vida privada, fruto da coleta desenfreada de dados, numa altura em que, para as empresas, o essencial já não é mais produzir bens, mas recrutar por todos os meios um parque de clientes.

A Internet pode ser definida, de forma sintética, como uma rede de computadores de caráter global, estruturada de modo a não depender de centros de controle para sua operação. Neste sentido, é uma tarefa bastante árdua obter o controle sobre o tráfego de dados, de modo a restringir o acesso a quem não diz respeito, haja vista que se compõem, essencialmente, de um "protocolo de comunicações, implementado em computadores, possibilitando sua interligação através dos vários meios de comunicação de dados existentes". (DONEDA, 2006, p. 58).

A transformação tecnológica proporcionada pela expansão da internet favoreceu ao aperfeiçoamento da forma como a gestão dos dados pode ser manipulada. Se no início da sociedade da informação se acreditava que os bancos de dados seriam uma das grandes ferramentas de controle dos dados e também de violação a direitos fundamentais, atualmente, a intervenção sobre a privacidade no que tange aos dados pessoais demonstra grande potencial de dano com a própria internet, possibilitando que o Estado ou o ente privado apenas necessite espionar uma determinada transmissão de dados realizada pelo indivíduo, obtendo as informações que pretende de forma secreta.

Danilo Doneda (2006, p. 171-172) chama a atenção para este fato:

> O advento da informática e as mudanças políticas e sociais que lhe são correlatas constituem um ponto de inflexão com consequências também para a ordem jurídica, cujo primeiro desafio é exatamente o de compreender o real efeito destas mudanças. [...] Alguns destes efeitos são mensurados quantitativamente, isto é, são decorrência

> do maior volume de informação que pode ser processado. Porém, não é somente a quantidade de informação processada que diferencia o tratamento informatizado de dados, mas também novos métodos, algoritmos e técnicas podem ser utilizados para este fim, operando igualmente uma mudança *qualitativa* no escopo do tratamento de dados pessoais.

E, de fato, inúmeras são as ferramentas utilizadas para o monitoramento indevido dos dados pessoais e da intimidade do indivíduo, muitas vezes à revelia do próprio Estado.

3.4.1 O *Profiling*

Uma das técnicas é conhecida como *profiling,* que consiste na elaboração de perfis de comportamento de um indivíduo ou grupos, tendo como ponto de partida as próprias informações disponibilizadas pelo consumidor. Nestes perfis os dados pessoais são estudados com a ajuda, por exemplo, de métodos estatísticos, técnicas de inteligência artificial entre outras, com o objetivo de se alcançar a "metainformação". (DONEDA, 2006, p. 173).

Com ela se torna possível sintetizar as preferências, os hábitos, os costumes e outros registros inerentes à rotina privada, cujas conclusões podem ser utilizadas indevidamente para se traçar uma análise comportamental dos indivíduos para a tomada de decisões estratégicas com o objetivo de aumentar o lucro empresarial.

E esta medida empresarial é capaz de reduzir a seara de atuação da liberdade individual e coletiva, considerando que a prévia análise dos dados fora capaz de antever o comportamento predefinido do cidadão, manipulando-o por meio do seu perfil virtual, única parte da personalidade visível.

3.4.2 O *Data Mining*

Há ainda o exemplo de outra técnica de coleta de dados pessoais chamada *data mining*, que também apresenta um potencial nocivo à proteção da privacidade dos consumidores. Com ela torna-se possível realizar uma "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". Basicamente, busca transformar informação em estado bruto em informação de potencial interesse. (DONEDA, 2006, p. 176).

Não se pode desconsiderar as consequências do manejo do *data mining,* pois, diante do grande número de informações em estado bruto disponível na rede mundial de

computadores, desde a troca de mensagens por e-mail, passando pelo monitoramento das pesquisas realizadas no navegador de busca do computador ou aos dados cadastrados em site quando realizada uma transação, está cada vez mais fácil obter uma informação útil sobre a vida privada do consumidor.

3.4.3 O *Data Warehouse*

Laura Shertel Mendes (2014, p. 108-109) acrescenta o *data warehouse* como mais uma técnica de tratamento e processamento dos dados. Trata-se de um sistema informatizado capaz de armazenar uma quantidade muito grande de informações, possibilitando a extração de relatórios e a leitura de uma grande base de dados complexos. Este sistema é caracterizado por não ser volátil, haja vista que os dados coletados não sofrem alteração. Organizam-se os dados pessoais dos consumidores junto aos inúmeros sistemas em operação, conforme a sua relevância, de modo a favorecer a tomada de decisão comercial estratégica em um futuro próximo. (MENDES, 2014, p. 108-109).

3.4.4 *Online Analytical Processing* (OLAP)

Podemos ainda citar o *Online Analytical Processing* (OLAP), que consiste em uma técnica que aperfeiçoa a técnica da mineração dos dados (*data mining*) e possibilita a análise dos dados existente em um *data warehouse*, que já é um banco de dados, permitindo uma análise muito mais ampla e multidimensional dos dados pessoais dos consumidores, tanto para realização de pesquisas quanto para a apresentação de informações. (MENDES, 2014, p. 110-111).

Trata-se de uma ferramenta muito útil para se acessar e analisar as informações já dispostas em determinada base de dados, atuando em alta performance de modo a auxiliar a tomada de decisões. Utilizar este processo para o confronto de diversos dados acerca da vida de um indivíduo possibilita se descobrir informações valiosas sobre o seu comportamento e os próximos passos da sua vida em sociedade, violando a sua privacidade.

3.4.5 O *Scoring*

Por derradeiro, identifica-se a técnica chamada *scoring.* Com o objetivo de identificar os “melhores consumidores”, a empresa se utiliza de um sistema de avaliação, pautada em

critérios objetivos, que sinaliza os clientes que tenham mais relevância para o negócio com o intuito de lhes oferecer promoções ou executar medidas para a sua fidelização. (MENDES, 2014, p. 112). Poder ser um modelo de escore de caráter comportamental ou para aprovação do credito. (SAUNDERS, 2000, p. 110).

No mesmo sentido é o entendimento de Ródnei Bernardino Souza, que define o *scoring*, ou simplesmente escore, como "o risco de inadimplência do tomador, ou seja, estima se o potencial usuário do cartão de crédito honrará os seus compromissos após iniciar a utilização do produto". (SOUZA, 2000, p. 22).

A técnica do *scoring* também é muito utilizada para avaliar históricos anteriores de compras e pagamentos a fim de identificar se o consumidor apresenta um baixo risco de inadimplência, podendo recusar bens e serviços a outros pretendentes de maior risco apenas levando em consideração um perfil pretérito de consumo.

Não podemos negar que o grande desenvolvimento experimentado pelo comércio eletrônico disponibiliza a todos grandes oportunidades, exigindo alguns mecanismos de segurança na realização de suas transações como usuário e senha, entretanto, muitos questionamentos podem ser direcionados à sua capacidade de oferecer garantias adequadas para a tutela da privacidade dos consumidores.

Partindo de uma perspectiva puramente liberal, entende-se que as relações privadas deveriam ser tuteladas e reguladas pelo próprio mercado, desonerando o Estado desta responsabilidade, contudo, "é preciso questionar se uma mudança tão radical deve ser confiada somente à dinâmica espontânea das formas do mercado" (RODOTÀ, 2008, p. 157), ou se caberia ao próprio Estado regular esta nova sociedade por meio do Direito e das políticas públicas.

De certo, em se tratando a privacidade de um dos atributos dos direitos da personalidade, a internet e o ciberespaço devem possibilitar a formação das qualidades intrínsecas do indivíduo promovendo a sua dignidade, contemplando o exercício da liberdade de expressão, da liberdade de associação e da sua intimidade, algo que não poderá ser atingido sem a construção de instrumentos legais específicos neste sentido, acompanhado de medidas em arranjos internacionais.

3.5 OS DADOS SENSÍVEIS

Como podemos concluir até então que nem todos os dados de determinado indivíduo são relevantes o suficiente para merecer a tutela jurídica contra aquele que os divulga. A cor do seu carro, a marca da roupa que veste, quantas vezes viajou no ano, são exemplos de situações que constituem dados, embora sem relevância jurídica.

Existem outros dados, os pessoais, que, entretanto, são mais específicos e retratam situações da vida privada e da intimidade dos indivíduos, e que são juridicamente tutelados pelo fato de serem inerentes à dignidade da pessoa humana e materializarem características fundamentais da personalidade.

Dentre os dados pessoais encontram-se os dados sensíveis, aqueles que atingem o núcleo fundamental da privacidade e referem-se a questões de cunho pessoal, tais como as raciais, as de gênero e opção sexual, as de saúde ou de escolha religiosa, por exemplo, bem como as informações sobre credo político ou os dados genéticos de um indivíduo. (DONEDA, 2006, p. 160-161).

De acordo com Laura Schertel Mendes (2014, p. 74),

> a categoria dos dados sensíveis está relacionada à percepção de que o armazenamento, o processamento e a circulação de alguns tipos de dados podem se constituir em um risco maior à personalidade individual, especialmente se utilizados com intuito discriminatório. Os dados referentes a raça, opção sexual, saúde e religião são exemplos desse tipo.

Danilo Doneda chama a atenção para o fato de que esta classificação da informação em subcategorias inter-relacionadas com questões da vida pessoal pode vir a causar a fragmentação e o enfraquecimento da tutela (DONEDA, 2006, p. 159-160), e uma consequente relativização de um direito em construção diante de uma sociedade tecnológica em plena expansão.

Contudo, o mesmo autor reconhece que os dados sensíveis são um produto da realidade prática da tutela dos dados pessoais e que não podia ser desconsiderada, haja vista que não se pode negar que exista uma diferença entre “o efeito do tratamento destes dados em relação aos demais”. (DONEDA, 2006, p. 161).

A denominação “dados sensíveis” surgiu diante da constatação de que as suas informações, quando veiculadas indevidamente, são amplamente capazes de proporcionar

grave lesão contra os seus titulares. Por conseguinte, os riscos do seu compartilhamento decorrem da grande possibilidade de serem utilizados com finalidades discriminatórias. (RODOTÀ, 2008, p. 96).

A Constituição Federal de 1988 elencou como um dos seus fundamentos a proteção à dignidade da pessoa humana, norma principiológica que irradia suas diretrizes, inclusive, às normas infraconstitucionais e às relações privadas. Não se pode tolerar que a personalidade do indivíduo seja violada pela manipulação indevida dos seus dados a fim de favorecer terceiros politicamente ou economicamente.

Não se pode perder de vista que os dados sensíveis já são objeto de proteção em outros ordenamentos pelo mundo, a exemplo da Europa, que prevê no art. 6º do Convênio 108 de 1981, de autoria do Conselho da Europa, que os dados pessoais relativos a origem racial, saúde, vida sexual e condenações penais somente poderiam ser objeto de tratamento na hipótese de previsão no direito interno de cada país. (COUNCIL OF EUROPA, 1981).

A previsão de tutela dos dados sensíveis também é objeto do art. 8° da Diretiva Europeia 95/46/CE, que também julgou prudente a limitação no processamento destes dados. Prevê o citado artigo que os países deverão proibir o tratamento dos dados considerados sensíveis. (COMUNIDADE EUROPEIA, 1995).

Não é demais salientar que este movimento mundial no sentido da proibição legal da coleta e do tratamento dos dados sensíveis, tanto pelo Estado quanto pela iniciativa privada, não pode ser considerado absoluto, tendo em vista que em algumas situações este recurso pode ser utilizado de forma legítima, quando, por exemplo, visa à compreensão do perfil social e demográfico de cada localidade, o que favorecerá a tomada de decisões políticas mais eficientes em prol do interesse público.

E neste sentido, conforme chama a atenção Danilo Doneda (2006, p. 163), o radicalismo nesta forma de pensar se mostra inviável, considerando que muitas instituições, sobretudo as públicas, poderiam ter suas funções comprometidas na eventual hipótese de se verem obstaculizadas ao acesso a alguns destes tipos de informação.

O importante é se viabilizar juridicamente ferramentas de controle sobre estes dados pessoais, e que a destinação dos mesmos seja apenas e tão somente em prol dos interesses da coletividade, responsabilizando aquele que as divulgar indevidamente, as compartilhar ou que as utilizar com finalidade discriminatória ou estigmatizante.

É necessário ponderar, entretanto, que não só os dados considerados "sensíveis" apresentam grande potencial de dano aos usuários da internet, pois, os dados pessoais (e não sensíveis), quando submetidos a um tratamento inadequado e mal intencionado, também podem revelar circunstâncias da intimidade e da personalidade de alguém, favorecendo o seu manejo para práticas discriminatórias. (DONEDA, 2006, p. 162).

Neste mesmo sentido é o pensamento de Helen Nissembaum (2010, p. 37-45), quando reconhece o potencial estigmatizante e discriminatório dos dados pessoais, sensíveis ou não sensíveis, quando manipulados indevidamente, evidenciando quatro transformações fundamentais no estágio histórico atual, no que tange à violação dos dados pessoais, sendo eles a ampliação da democratização das redes e dos bancos de dados, da facilidade de divulgação da informação, da mesma informação agregada e, ainda, o conhecimento que se pode auferir a partir destas informações.

A autora ainda defende o que chama de "integridade contextual" (NISSEMBAUM, 2010, p. 48), que pode ser caracterizada como algo que vai além da mera proteção ao sigilo das pessoas ou da necessidade do autocontrole sobre os seus dados, passando pelo direito a um fluxo adequado das informações privadas, orientado conforme as previsões de proteção constantes das normas internacionais, visto que são orientadas a partir das necessidades e dos contextos sociais.

Oportuna é a lição de Stefano Rodotá, no que tange à esfera última da privacidade e a sua correlação com os dados sensíveis:

> o "núcleo duro" da privacidade é ainda hoje constituído por informações que refletem a tradicional necessidade de sigilo (por exemplo, aquelas relacionadas à saúde ou aos hábitos sexuais): internamente, porém, assumiram cada vez maior relevância outras categorias de informações, protegidas sobretudo para evitar que pela sua circulação possam nascer situações de discriminação, com danos aos interessados. (RODOTÁ, 2008, p. 95-96).

A omissão do ordenamento jurídico brasileiro em regulamentar a tutela dos dados pessoais em norma específica, sobretudo no que tange aos dados sensíveis, manifesta uma situação extremamente temerária ao indivíduo, por possibilitar que suas informações mais íntimas e peculiares sejam coletadas, armazenadas e eventualmente utilizadas, violando a prerrogativa da dignidade da pessoa humana.

Sem dúvida, a real possibilidade de se manter um controle efetivo sobre as suas próprias informações pessoais, seja no ambiente real ou no virtual, contribui de forma

determinante para enquadrar o indivíduo como um sujeito de direitos, contribuindo para se estabelecer o lugar do cidadão na sociedade.

4 A PROTEÇÃO DOS DADOS PESSOAIS NO DIREITO COMPARADO

4.1 A ORIGEM EUROPEIA DA PROTEÇÃO AOS DADOS PESSOAIS

Como fora construído até aqui, a proteção à privacidade dos indivíduos é um movimento relativamente novo na história da humanidade, haja vista que a sociedades antigas não eram consideradas tão complexas como as atuais, não evidenciando a necessidade de tutela deste interesse.

O avançar da história impôs aos homens muitos séculos de subjugação aos impérios, a exemplo do que ocorreu durante toda a Idade Média, de modo que não se cogitava em qualquer tipo de garantia de proteção à vida, à saúde ou à integridade física de nenhum indivíduo, muito menos da privacidade.

Entretanto, os novos sopros libertários dos séculos XIX e XX iniciaram uma fase histórica de mudança no que tange à proteção à liberdade do indivíduo, à sua autonomia e, consequentemente, à vida privada e à intimidade dos indivíduos. E a transformação neste paradigma partiu também dos arranjos institucionais germinados no âmbito internacional.

É o momento do surgimento da sociedade da informação, caracterizada pela expansão tecnológica e pela criação de ferramentas que favoreceram a difusão do conhecimento e da comunicação entre os povos, aproximando línguas, culturas e tradições. Entretanto, cabe mencionar que esta sociedade é dinâmica e complexa, manifestando sempre o potencial de expansão e readaptação com os valores cultuados pela comunidade.

E com esta mesma sociedade que fomenta a interação entre os indivíduos e o acesso rápido às informações sobre o que ocorre a cada momento no planeta, surgem novos desafios à promoção dos direitos fundamentais, sobretudo no que tange à proteção da privacidade e aos dados pessoais, sobretudo com a difusão da internet.

Apesar de a soberania nacional ser um fundamento básico para toda e qualquer nação, a ampla expansão tecnológica e globalizatória torna as fronteiras entre os Estados mais fluidas. (COHEN, 2003, p. 430). As informações são compartilhadas pela internet para qualquer parte do planeta em tempo real, em um fluxo intenso de dados que exigem que a tomada de decisão mais sensata sobre a proteção aos dados pessoais surja a partir de arranjos internacionais, de forma comunitária, envolvendo todos os prejudicados.

Neste sentido é o entendimento de Stefano Rodotá (2008, p. 63-64), quando defende que a criação de um diploma normativo internacional para a proteção da informação na era digital deve ser visto como um aspecto específico de uma política global da informação, disciplinando de forma mais ampla as inúmeras possibilidades de violação à proteção dos dados, sobretudo no que tange às questões envolvendo os bancos de dados transnacionais, que estão alheios ao controle dos Estados nacionais.

4.1.1 As gerações de Leis de Proteção aos dados pessoais

As primeiras experiências de produção normativa contra a coleta, armazenamento e compartilhamento indevido dos dados pessoais surgem na década de 1970, com a Lei do Land Hesse de 1970, na Alemanha, sendo seguido do Estatuto para bancos de dados de 1973 (*Data Legen*), na Suécia, e passando pelo *Privacy Act* norte-americano de 1974, década onde surgiu a "primeira geração" (DONEDA, 2006, p. 206-207) das leis de proteção aos dados pessoais.

Tais diplomas normativos surgiram com o objetivo de regular uma conjuntura social onde se buscava impedir que os grandes centros elaboradores de dados concentrassem a coleta, o armazenamento e a gestão dos dados pessoais. O que se pretendia essencialmente com estas leis era "a concessão de autorizações para a criação destes bancos de dados e o seu controle *a posteriori* por órgãos públicos". (DONEDA, 2006, p. 208).

Contudo, diante da velocidade em que ocorre a expansão tecnológica, novos desafios logo se apresentaram, quando então estas normas já passaram a se tornar ultrapassadas. O motivo preponderante fora que o desenvolvimento de uma ampla capacidade de processamento de dados tornou ineficaz um sistema tradicional de controle e emissão de autorizações baseado em procedimentos rígidos e detalhados que demandavam o acompanhamento detalhado. (DONEDA, 2006, p. 209).

Já no final da década de 1970, surge a chamada "segunda geração" (DONEDA, 2006, p. 209) de leis sobre a matéria, tendo como principal fato gerador a expansão desenfreada dos bancos de dados informatizados. Neste contexto nascem em 1978, por exemplo, a lei francesa de proteção de dados pessoais, também chamada *Informatique et Libertées*.

Pode-se compreender que as leis germinadas neste período histórico apresentam características básicas que as diferenciam das anteriores, sobretudo, pela sua estrutura, que já não mais direcionam atenção ao fenômeno computacional em si, mas sim, foca na privacidade

e na proteção do fluxo dos dados pessoais enquanto uma liberdade negativa do indivíduo, sujeito de direitos. (DONEDA, 2006, p. 209).

Refletiu um momento histórico onde os cidadãos não mais toleravam os incômodos gerados pela coleta, armazenamento e utilização indevida dos seus dados pessoais por parte de terceiros, sobretudo com a vida no mundo digital, o que passou a se exigir uma atenção especial do Estado e a consequente garantia de instrumentos legais para a defesa destes interesses.

Entretanto, Danilo Doneda chama a atenção para os problemas que emergiram com as leis de segunda geração de proteção aos dados pessoais na Europa:

> 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. Tanto o Estado como os entes privados utilizavam intensamente o fluxo de informações pessoais para seu funcionamento, e a interrupção ou mesmo o questionamento deste fluxo pelo cidadão [...] implicava não raro na sua exclusão de algum aspecto da vida social, ou em algum tipo de prejuízo mensurável. (DONEDA, 2006, p. 210).

De fato, muito difícil será ao usuário manter-se em sigilo quando conectado à rede mundial de computadores, sobretudo porque o ingresso na vida digital pressupõe o prévio cadastramento dos seus dados pessoais, sendo vedado o anonimato, o que já é suficiente para ser identificado como uma ferramenta de coleta questionável. Recusar-se a esta exigência é o mesmo que proceder à exclusão do indivíduo à sua "cidadania virtual", proporcionando obstáculos ao desenvolvimento da sua dignidade.

Entretanto, um novo movimento de aperfeiçoamento surge ainda na Europa na década de 1980, refinando a tutela dos dados pessoais, a exemplo da decisão proferida pelo Tribunal Constitucional Alemão (BVefGE 65, 1, Volkszählung), que julgou inconstitucional parte da Lei do Censo e que induziram a emendas às leis de proteção de dados na Alemanha em 1990 e na Áustria 1986, bem como culminaram em novas leis pela Europa. (DONEDA, 2006, p. 211). São conhecidas como a "terceira geração de leis" (Idem) de proteção aos dados pessoais na Europa, onde o foco concentrado no cidadão permanece, porém, amplia-se para além da liberdade de fornecer ou não os dados pessoais, visando também garantir a plena efetividade desta liberdade.

Com a alteração do contexto tecnológico, novos desafios foram impostos à tutela da privacidade, haja vista que se deixou de ser necessária a localização física dos bancos de

dados, haja vista que passaram a serem armazenados em redes e não mais em um dispositivo centralizados de processamento de dados, que passaram à capacidade de serem transferidos em altíssima velocidade. (MAYER-SCHÖNBERGER, 2001, p. 230).

Nesta geração de leis, a proteção dos dados é materializada por meio de diplomas legais dotados de um pouco mais de complexidade e que consideram a posição ocupada pelo cidadão em sociedade, mas também, "o contexto no qual lhe é solicitado que revele seus dados", favorecendo o surgimento de meios adequados para toda a ocasião em que a liberdade de decidir é cerceada sob determinadas condições, violando o exercício da "autodeterminação informativa" do cidadão. (DONEDA, 2006, p. 211).

O momento posterior à década de 1980 é o terreno da "quarta geração" das leis de proteção aos dados pessoais dos indivíduos, germinadas pelas inovações tecnológicas trazidas pela expansão tecnológica da década de 1990 e seguintes, que, de acordo com Danilo Doneda (2006, p. 212), "caracterizam-se por procurar suprir as desvantagens do enfoque individual" analisando o problema da informação através da necessidade de instrumentos para a defesa coletiva destes direitos.

4.1.2 As Diretrizes da OCDE sobre a Proteção da Privacidade e do Fluxo Transnacional de Dados Pessoais (1980)

Em meio a este movimento global em busca da proteção à privacidade e aos fluxos transfronteiriços dos dados pessoais dos indivíduos, surgem as diretrizes da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) por volta da década de 1980, de modo a conduzirem uma política internacional de proteção.

As Diretrizes ou "*Guidelines"* sobre a privacidade, que entraram em vigor em 23 de setembro de 1980, simbolizam um consenso internacional quanto à necessidade de tutela dos dados pessoais, bem como no que tange à coleta e monitoramento destas informações, inclusive, elencando princípios orientadores a serem implementados em maior grau possível, de modo a prevenir violação aos direitos humanos fundamentais.

Em que pese as Diretrizes vigorarem a partir de 1980, os estudos sobre o tema já iniciaram desde 1978, quando a OCDE criou um grupo de trabalho composto de especialistas em tráfego transnacional de dados, com objetivo de sugerir um diploma legal sobre o assunto que pudesse servir de padrão internacional.

O objetivo proposto durante os trabalhos fora identificar a melhor forma de ampliar o manejo da informática sem que tal medida pudesse prejudicar a privacidade das pessoas. Como resultado, fora elaborada uma Recomendação ao Conselho da OCDE, materializadas por meio das *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[2], que passaram a vigorar em 1980 aos Estados membros.

Danilo Doneda (2006, p. 230-231) evidencia alguns dos problemas que podem ser identificados na abordagem dada pela OCDE ao tema. A maior preocupação materializada na elaboração das diretrizes fora com o tráfego de dados e não com sua proteção, ou seja, desprezando a preocupação principal com a tutela das pessoas.

Ademais, o autor chama a atenção para o fato de que as recomendações oriundas do Conselho da OCDE não são taxativas tampouco vinculantes, o que significa que os países-membros não estão obrigados a produzirem legislações nacionais conforme as "*Guidelines"*, não exercendo qualquer influência sobre o direito interno destas nações. (DONEDA, 2006, p. 230-231).

Por derradeiro, Doneda (2006, p. 231) ainda menciona mais um motivo identificado com a vigência das Diretrizes, o que contribuiu para a sua relativização. No ano seguinte, em 1981, o Conselho da Europa passou a regular o fluxo dos dados pessoais através da Convenção nº 108, constituindo uma das primeiras iniciativas em prol da criação de um sistema integrado de proteção aos dados pessoais na Europa.

4.1.3 A Convenção de Strasbourg nº 108 do Conselho Europeu (1981)

Trata-se do primeiro texto unificado onde se pretendeu regular juridicamente por completo a matéria envolvendo a proteção dos dados pessoais.

Em 28 de janeiro de 1981, na cidade de Strasbourg, França, em reunião do Conselho Europeu, fora editada a Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais de nº 108[3], que procurava estimular os Estados-membros a adotarem estas diretrizes como padrão para normas específicas para a coleta e tratamento dos dados pessoais. (COUNCIL OF EUROPA, 1981).

---

[2]http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm - acesso em: 10 jan. 2017.

[3]https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37 – acesso em: 20 jan. 2017.

Passando a vigorar apenas em 1985, a Convenção nº 108 tinha por objetivo tutelar direitos específicos do indivíduo que deveriam estar assegurados contra a liberdade de transmissão das informações e dos dados pessoais para além das fronteiras nacionais.

Já no seu artigo 1º, assegurou a cada um "o respeito de seus direitos e liberdades fundamentais e em particular do seu direito à vida privada, em relação à elaboração automática dos dados pessoais que lhe dizem respeito[4]". Logo se seguida, no art. 3º, deixa evidente que as disposições são aplicáveis tanto ao setor público quanto ao privado. (COUNCIL OF EUROPA, 1981).

Em todo o seu teor, a Convenção nº 108 do Conselho Europeu poderia ser dividida em três partes fundamentais, sendo a primeira aquela destinada aos princípios básicos, a segunda direcionada à disciplina de regras especiais no que tange ao fluxo transnacional de dados pessoais e, em terceiro, disciplina os mecanismos de entrada dos dados e da consulta pelos interessados. (LIMBERGER, 2007, p. 68).

Entretanto, o Convênio fora elaborado na forma de recomendação aos Estados-membros e, apesar de se materializarem em diretrizes importantes para a tutela dos dados pessoais por parte das nações europeias, apresentou a mesma fragilidade encontrada em relação às *guidelines* da OCDE: o seu caráter não vinculante.

Ainda assim, podemos dizer que a Convenção atingiu parte dos seus objetivos, haja vista que incentivou o surgimento de diversas legislações nacionais dos Estados europeus, bem como atuou como diretriz orientadora sobre o tema.

Como consequência, no dia 8 de dezembro de 1992 a Bélgica aprovou sua primeira lei sobre a proteção dos dados pessoais. No ano seguinte, em 31 de janeiro de 1993, foi a vez da Espanha e, no ano de 1984, o Reino Unido promulga o *Data Protection Act*. (DONEDA, 2006, p. 232).

4.1.4 A Diretiva Europeia 95/46/CE (1995)

Um dos grandes problemas enfrentados pelos Estados no que tange à proteção dos dados pessoais está no fato de que a previsão normativa exclusiva do direito interno das nações se mostra insuficiente, haja vista que o cenário tecnológico atual faz com que os dados

[4]https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37 – acesso em: 20/01/2017.

e as informações ultrapassem as fronteiras dos Estados, exigindo uma padronização mínima no cenário internacional.

Neste sentido surge a Diretiva Europeia n° 95/46/CE[5] do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, passando a regular a proteção dos indivíduos no que tange ao tratamento dos dados pessoais e a livre circulação destes mesmos dados e informações.

Têmis Limberger destaca a diferença existente entre a Diretiva 95/46 e o Convênio nº 108 do Conselho Europeu. Para o autor, a primeira não se presta à persecução da proteção dos indivíduos em relação aos perigos na manipulação inadequada dos dados, mas sim, "permitir a livre circulação dos dados." (LIMBERGER, 2007, p. 66).

No artigo 3º da Diretiva há previsão expressa no que tange ao campo de incidência da norma. Segundo texto legal, a Diretiva teria aplicação a todo e qualquer tratamento automatizado de dados pessoais, podendo ou não estar contidos em cadastros. Como consequência, estaria excluída da sua competência a coleta e tratamento dos dados não automatizados.

Entretanto, cabe evidenciar que no mesmo artigo, mais precisamente no item 2, restou evidenciada a não aplicação da Diretiva às situações envolvendo a segurança pública, a defesa e a segurança do Estado, bem como no que tange às questões envolvendo a persecução criminal.

A sua interpretação deixa claro que o direito à privacidade no que tange à tutela dos dados pessoais dos indivíduos não é um direito absoluto, mas sim, relativo, por permitir a sua restrição nas circunstâncias mencionadas. Entretanto, não se pode tolerar que a violação deste direito esteja fundamentada em uma justificativa de segurança do Estado pautada em premissas falsas, o que incentivaria uma espionagem institucional.

4.1.5 A Diretiva Europeia 97/66/CE (1997)

A Diretiva 95/46/CE fora complementada pela Diretiva Europeia 97/66/CE[6] do Parlamento Europeu e do Conselho de 15 de dezembro de 1997, que propõe a tutela relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das telecomunicações.

[5] http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_pt.pdf - acesso em: 01 fev. 2017.
[6] http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31997L0066&from=PT – acesso em: 30 jan. 2017.

Buscando proteger a confidencialidade das comunicações, o artigo 5º da referida Diretiva previu a obrigação dos Estados-membros garantirem normas jurídicas protegendo a confidencialidade dos dados e das comunicações do usuário contra o acesso de terceiros, exceto mediante autorização judicial.

No artigo 6º, ao tratar do tráfego de dados e da sua faturação, a Diretiva 97/66/CE previu que os fornecedores do serviço de telecomunicações devem apagar ou tornar anônimo os dados de tráfego dos assinantes logo após a conclusão da chamada. Trata-se de uma medida importante na proteção da intimidade das pessoas que pode, inclusive, servir de exemplo para o legislativo brasileiro.

Uma questão de suma relevância no que tange à proteção aos dados pessoais fora contemplado nesta Diretiva e se refere à questão do consentimento do usuário. Segundo o mesmo artigo 6º, para fins de comercialização dos próprios serviços de telecomunicações, somente será autorizada o eventual tratamento dos dados pessoais na hipótese estrita de haver o consentimento do usuário.

Assim como em todos os diplomas normativos internacionais mencionados nos itens anteriores deste trabalho, há também na Diretiva 97/66/CE, no seu artigo 14, a previsão de que os Estados-membros estão autorizados a criar medidas restritivas às garantias deste direito diante da necessidade de salvaguardar a segurança do Estado, a defesa e a segurança pública, bem como na hipótese de persecução criminal. (EUROPA, 1997).

4.2 OS PRINCÍPIOS DE PROTEÇÃO AOS DADOS PESSOAIS

A partir da interpretação conjugada de todos estes diplomas normativos oriundos do continente europeu, é possível se extrair um rol de princípios fundamentais no que tange à proteção dos dados pessoais, que poderão servir de referência aos demais Estados onde tal temática ainda não é retratada no seu direito interno, como é o caso do Brasil.

Os princípios são identificados através da conjugação das disposições constantes da Recomendação da OCDE de 1980, da Convenção nº 108 do Conselho da Europa de 1981, e, ainda, das previsões inseridas nas Diretivas Europeias 95/46/CE e 97/66/CE.

Estes princípios possuem a finalidade de impor restrições à coleta, ao tratamento e ao compartilhamento dos dados pessoais dos indivíduos, bem como são direcionados à limitação

do poder do Estado e das empresas privadas e, em contrapartida, atribuem poder ao indivíduo para o autocontrole do fluxo de transmissão dos próprios dados. (MENDES, 2014, p. 68).

Na parte II das *Guidelines* da OCDE se descreve alguns dos princípios básicos inerentes à proteção à privacidade e aos dados pessoais.

Conforme o *Princípio da Limitação da Coleta*, a coleta dos dados pessoais deveria ser limitada e quaisquer dos dados coletados deveriam ser obtidos somente através dos meios justos e legais e, sempre que possível, informando e pedindo o consentimento do titular dos dados. (OCDE, 2002, p. 4).

Evidencia-se o P*rincípio da Qualidade dos Dados.* Neste caso, os dados pessoais deveriam ser relacionados estritamente com as finalidades de sua utilização e na exata medida da sua necessidade, devendo ser exatos, completos e permanentemente atualizados. (OCDE, 2002, p. 4).

Danilo Doneda chama de "Princípio da exatidão", onde os dados armazenados devem manter-se fiéis à realidade e à necessidade da sua coleta. Por conseguinte, o tratamento dado deve contemplar medidas de segurança bem como serem realizadas periódicas atualizações destes dados, de acordo com a necessidade. (DONEDA, 2006, p. 216).

Acrescenta Laura Mendes (2014, p. 71-72) que "para a efetividade do princípio da qualidade dos dados, é fundamental a garantia dos *direitos de acesso, retificação e cancelamento dos dados*".

Segundo o *Princípio da Definição da Finalidade*, as intenções pela coleta dos dados pessoais devem ser mencionadas logo no momento da sua coleta, sendo que o uso subsequente estaria vedado enquanto não respeitado este dever. Na hipótese de alteração do propósito original, o usuário deverá ser cientificado afim de que possa manifestar sua concordância, se assim o desejar. (OCDE, 2002, p. 4).

Stefano Rodotá (2008, p. 59) acrescenta que a correlação entre os dados pessoais colhidos e a estrita finalidade deve contemplar a pertinência (princípio da pertinência), bem como a adequação entre a finalidade e a utilização dos dados não pode ser abusiva (princípio da utilização não-abusiva).

Acrescenta ainda o autor que, segundo este princípio, os dados pessoais e as informações desnecessárias ou desvirtuadas da sua finalidade deverão ser eliminadas ou

transformados em dados anônimos (princípio do direito ao esquecimento). (RODOTÀ, 2008, p. 59).

No que se refere ao *Princípio da Limitação da Utilização*, restou consignada a vedação à divulgação, à comunicação ou à utilização dos dados pessoais dos indivíduos com finalidades diversas das que foram especificadas, exceto se detiver o consentimento do titular dos dados ou por força de lei. (OCDE, 2002, p. 4).

De acordo com o *Princípio do Back-up de Segurança*, também chamado de "Princípio da segurança física e lógica" (DONEDA, 2006, p. 217) (RODOTÀ, 2008, p. 59), é defendido pelas Diretrizes da OCDE a realização de *back-ups* de segurança frequentes no intuito de proteger os dados pessoais dos cidadãos contra os riscos da perda, da destruição, do uso, da modificação ou da divulgação não autorizada dos dados pessoais. (OCDE, 2002, p. 5).

Segundo o *Princípio da Abertura ou da Publicidade*, deveria haver uma política geral de abertura a respeito do desenvolvimento, da prática e da política inerente aos dados pessoais, assegurando que os mesmos estejam disponíveis aos titulares, bem como que fossem estabelecidas as principais finalidades para o seu uso, além da identidade e da residência habitual do controlador dos dados. (OCDE, 2002, p. 5).

Também chamado de "princípio da publicidade" (RODOTÀ, 2008, p. 59) ou de "princípio da transparência" (MENDES, 2014, p. 71), exige que a existência de qualquer banco de dados destinado ao armazenamento de informações sobre os indivíduos deva ser de conhecimento público.

Ademais, torna-se necessário exigir a prévia autorização governamental para funcionamento dos bancos de dados, bem como a apresentação de relatórios periódicos de avaliação acerca da segurança das informações. (DONEDA, 2006, p. 216).

Já em relação ao *Princípio da Participação do Indivíduo ou Princípio do Acesso* Individual, visa assegurar o direito de todo indivíduo: de obter daquele que controla os dados a confirmação de que o mesmo possui ou não dados referentes ao requerente; que lhe sejam comunicados a coleta dos dados em um prazo razoável, por um preço justo, de maneira razoável e de modo compreensível. (OCDE, 2002, p. 5).

Por conseguinte, este princípio ainda tem por objetivo garantir o direito do indivíduo de obter explicações acerca do motivo pelo qual teria havido o pedido de recusa do controlador dos dados e, por fim, o direito de contestar os dados relacionados ao próprio titular, bem como exigir que sejam apagados ou retificados. (OCDE, 2002, p. 5).

É também chamado de “princípio do acesso individual”, ou ainda “princípio do livre acesso” (DONEDA, 2006, p. 217), e respalda o direito do indivíduo de conhecer quais foram as informações coletadas sobre si próprio, bem como de exigir sua cópia, a correção daquelas informações equivocadas ou incompletas ou, ainda, a exclusão daquelas ilegitimamente coletadas. (RODOTÀ, 2008, p. 59).

De acordo com o *Princípio da Responsabilização*, o controlador dos dados pessoais responde pessoalmente pela má destinação dada aos dados mantidos sob seu controle ou pela violação de quaisquer dos princípios já elencados. (OCDE, 2002, p. 5).

4.3 A EXPERIÊNCIA DE ALGUMAS DAS LEIS DE PROTEÇÃO DOS DADOS PESSOAIS NA EUROPA

Com a expansão internacional deste movimento em prol da proteção do direito à privacidade do indivíduo, o que inclui os seus dados pessoais enquanto extensões do seu direito à personalidade, diversas tentativas de estabelecer diplomas legais de âmbito transnacional não atingiram muito dos seus objetivos, entretanto, influenciaram a produção legislativa interna dos Estados europeus.

4.3.1 A Evolução das Leis de Proteção aos Dados Pessoais na Alemanha

A Lei do Land Hesse Alemão de 7 de outubro de 1970 é o primeiro texto legal de proteção aos dados pessoais a vigorar em uma nação da Europa. Entretanto, alguns anos mais tarde, entra em vigor na Alemanha a Lei Federal de Proteção de Dados, datada de 27 de janeiro de 1977, passando a regular o cadastro de informações constantes junto a empresas públicas ou privadas. (LIMBERGER, 2007, p. 86).

Diante da expansão tecnológica e dos novos desafios experimentados pela sociedade do século XXI, surge a necessidade de atualização normativa, quando então fora promulgada a nova Lei Alemã de proteção aos dados pessoais em 20 de dezembro de 1990 (Bundesdatenschutzgesetz – BDSG).

Preenchendo algumas das lacunas existentes nos ordenamentos anteriores, embora não exaurindo o tema, a nova lei não altera substancialmente as previsões até então dispostas. Entretanto, a mudança destacável fora em relação ao bem jurídico protegido, que fora

expandido à proteção específica dos dados pessoais contra as potenciais arbitrariedades em relação ao armazenamento ou compartilhamento dos dados. (LIMBERGER, 2007, p. 88-89).

4.3.2 A Lei Francesa 78-17 de 1978

Na França, a proteção aos dados informatizados se dá mediante a Lei 78-17 de 6 de janeiro de 1978, uma das primeiras no mundo a tratar da proteção dos dados pessoais (BELLEIL, 2002, p. 78), e regulamentado pelo Decreto de 17 de julho de 1978.

A Lei Francesa contemplou princípios e definições semelhantes às previsões dos tratados internacionais. Entretanto, o diploma passou a dispor que a coleta, tratamento e conservação dos dados atendiam a três diretrizes fundamentais, sendo a primeira, no sentido de que os dados registrados devem guardar pertinência com a sua finalidade original. (LIMBERGER, 2007, p. 88-92).

A segunda diretriz diz respeito ao tempo de duração das informações coletadas, que não deverão sem mantidas por mais tempo do que o necessário e, por fim, a terceira diretriz prevê a exigência de disponibilização de instrumentos para a proteção dos dados sensíveis (LIMBERGER, 2007, p. 88-92), pois, quando violados, atingem as prerrogativas mais íntimas da personalidade do indivíduo.

4.3.3 A Lei Italiana n° 675 de 1996

Na Itália, surge a Lei nº 675 de 31 de dezembro de 1996, atuando como um estatuto geral sobre a informação. Indo além da adequação às diretrizes europeias, a lei italiana inovou ao prever tutela das informações inerente tanto à pessoa individual como à pessoa coletiva, pondo seus interesses no centro do ordenamento. (LIMBERGER, 2007, p. 96-97).

4.3.4 A Lei Portuguesa n° 67 de 1998

No caso de Portugal, vigora a Lei n° 67/1998[7] de proteção de dados pessoais, que, basicamente, transpôs para a ordem jurídica interna as previsões da Diretiva nº 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995.

[7] https://www.cnpd.pt/bin/legis/nacional/lei_6798.htm - acesso em: 5 fev. 2017.

O princípio geral adotado nesta lei fora no sentido de que a coleta e o tratamento de dados pessoais devem processar-se de forma transparente e lúcida possível, bem como no estrito respeito pela reserva da vida privada e aos direitos, liberdades e garantias fundamentais.

A preocupação com a qualidade dos dados coletados também se fez presente no texto da lei portuguesa, mais precisamente no seu artigo 5º. Segundo ele, os dados pessoais devem ser tratados de forma lícita e de boa-fé, atendendo a sua finalidade precípua, bem como serem utilizados e descartados quando não mais necessários.

No seu artigo 7º, a lei portuguesa proíbe o tratamento dos dados sensíveis, que são aqueles dados pessoais inerentes às convicções políticas ou filosóficas, ou a filiação partidária ou sindical, questão relacionada à fé, à vida privada e à origem racial ou étnica, bem como o tratamento de dados relativos ao estado de saúde e à vida sexual dos indivíduos, estando aí incluídos os dados genéticos.

Um ponto de suma importância constante do diploma português é a previsão dos direitos inerentes aos titulares dos dados pessoais coletados. De acordo com o artigo 10º, sempre quando houver a coleta de dados, o responsável pelo tratamento deverá informar o usuário apresentando a sua identificação e a finalidade.

Em seguida, o seu artigo 11º dispõe sobre o direito de acesso do titular dos dados pessoais, lhe assegurando a prerrogativa de obter junto ao responsável pelo tratamento dos dados, a confirmação se dispõe ou não os dados do usuário, bem como o pedido de retificação quando equivocados ou excluídos quando ilegitimamente coletados.

4.4 A PROTEÇÃO AOS DADOS PESSOAIS NOS ESTADOS UNIDOS

4.4.1 Considerações sobre o Sistema Jurídico Norte-Americano

Para melhor compreensão de como se dá a tutela da privacidade e dos dados pessoais no direito norte-americano, torna-se necessário tecer breves considerações acerca de como se estrutura o seu sistema jurídico, pautado sobre a *common law*.

Há uma grande dicotomia em relação aos dois dos mais importantes sistemas jurídicos contemporâneos, de um lado, o sistema romano-germânico, também conhecido por *civil law* e, de outro, o sistema da *common law* norte-americana, de origem anglo-saxã.

Em que pese o aprofundamento do estudo destes sistemas fuja ao propósito deste trabalho, não se poderia deixar de mencionar a característica fundamental que os define. No sistema romano germânico, onde integra a maior parte dos países da Europa e da América Latina, como o Brasil, a lei é erigida ao posto de fonte primária do Direito, priorizando-se a sua disposição em textos escritos codificados.

Já no caso norte-americano, assim como no inglês, o direito é essencialmente de cunho jurisprudencial, disposto por um corpo de direito não escrito. As regras de direito são declaradas pelos tribunais diante da decisão de um caso concreto (RENÉ DAVID, 2002, p. 463), servindo como precedente diretivo às eventuais demandas futuras. As leis escritas existem, contudo, em menor proporção.

Entretanto, em sede de Direito Comparado, não seria prudente se realizar juízos de valor do tipo "é melhor" ou "é mais eficaz". Conforme salienta Guido Soares, ambos os sistemas conservam suas peculiaridades e cumprem com sua finalidade, estruturando os valores fundamentais das sociedades em que foram elaboradas. (GUIDO SOARES, 2000, p. 15).

Desta forma, a *Common Law* norte-americana apresenta a sua principal característica, qual seja, o seu pragmatismo. (GUIDO SOARES, 2000, p. 12). Contudo, com exceção do Estado da Louisiana, o direito dos Estados Unidos é considerado como integrante de uma *common law* mista, por guardar algumas similitudes com o *civil law*. (Idem, p. 26).

Neste mesmo sentido é o entendimento de René David:

> A *common law* conserva hoje a sua estrutura, muito diferente da dos direitos romano-germânicos, mas o papel desempenhado pela lei foi aí aumentando e os métodos usados nos dois sistemas tendem a aproximar-se; sobretudo a regra de direito tende, cada vez mais, a ser concebida nos países de *common law* como o é nos países da família romano-germânica. (René David, 2002, p. 26).

E esta é uma tendência moderna, justificando que o jurista se desprenda de qualquer posicionamento radical quanto ao assunto. Estes sistemas, ainda que apresentem diferenças fundamentais, também são influenciados pela própria expansão da sociedade da informação, o que permite o afloramento dos pontos de conexão entre ambos.

Tanto a jurisprudência quanto a legislação podem ser consideradas como fontes do direito norte-americano, sendo que o sistema é pautado em uma constituição escrita. Entretanto, diante de um caso concreto, prevalecem as decisões judiciais sobre os textos legais infraconstitucionais, atuando como precedente.

Desta forma, veremos como surge a construção do *right do privacy* na *common law* norte-americana, abordando algumas das suas leis escritas que procuram tutelar este interesse fundamental.

4.4.2 A Construção do *Right to Privacy* nos EUA

Antes do século XIX, o direito à privacidade não era tutelado de forma direta pelos sistemas jurídicos, na medida em que a falta de complexidade da sociedade da época e a submissão do homem aos impérios, não exigiam a elaboração de uma norma jurídica sobre a proteção da intimidade e a vida privada das pessoas.

Contudo, a evolução histórica do direito à privacidade ou *right to privacy* no direito norte-americano surge a partir da construção doutrinária exposta por Samuel Warren e Louis D. Brandeis no artigo intitulado *The right to privacy,* publicado em 1890 na *Harvard Law Review*.

O pensamento exposto por Warren e Brandeis fora capaz de consolidar um ponto chave na construção histórica da privacidade, e consiste no reconhecimento da "*inviolate personality*": *The principle which protects personal writings and other personal productions, not against theft and physical appropriation, but against publications in any form, is in reality not the principle of private property, but that of an inviolate personality*. (WARREN; BRANDEIS, 1890, p. 196).

Nesta obra, os autores discutem a invasão da privacidade por conta da atuação de fotógrafos e jornalistas que devassavam a vida privada das pessoas e expunham a sua intimidade ao público. Na construção da sua tese, os autores evidenciaram que o gozo do direito à vida passou a ser evoluído para o direito de aproveitar a vida (*right to enjoy life*), e, por conseguinte, para o direito de ser deixado em paz (*the right to be let alone*).

A evolução deste pensamento culmina com o reconhecimento de um direito geral à privacidade:

> A partir da análise dos precedentes, documentou-se o reconhecimento na *common law* de um direito geral à *privacy*, reconstruível através dos casos de violação de propriedade (*property)*, violações da confiança (*breach of confidence*), violações do direito de autor (*copyright)* e também dos casos de difamação (*defamation)*. A conclusão a que chegaram foi de que, através do direito geral à *privacy*, era possível obter uma proteção jurídica também no caso de a violação da vida privada ocorrer por meio da imprensa. (LIMBERGER, 2007, p. 55).

Pode-se compreender que esta funcionalidade expandida é um reflexo do reconhecimento da privacidade enquanto questão fundamental para a democracia e para a liberdade norte-americanas. (DONEDA, 2006, p. 264). Neste sistema, o *right to privacy* seria essencialmente uma prerrogativa do cidadão perante o próprio Estado, regulando a ação do governo e não dos indivíduos. (DONEDA, 2006, p. 276).

Na perspectiva de Danilo Doneda, o *"right to privacy"*, embora não previsto expressamente na Constituição de 1787, está fundamentado na 1ª, 4ª e 14ª emendas da Constituição Americana, e é o que mais se aproxima da tutela dos dados pessoais. Assim, a concepção do sigilo e do isolamento fora transformado em um interesse de natureza pessoal, favorecendo o surgimento da tutela dos dados pessoais. (DONEDA, 2006, p. 284).

Acrescenta o autor:

> o *right to privacy* foi ou é evocado para regular a tranquilidade no próprio lar, o controle sobre informações pessoais, o controle sobre a vigilância, a proteção da reputação, a proteção contra averiguações e interrogatórios abusivos, o planejamento familiar, a educação dos próprios filhos, o aborto, a eutanásia, entre outros. (DONEDA, 2006, p.264).

Esta ampla funcionalidade é reflexo do reconhecimento da privacidade como questão fundamental para a liberdade e a democracia norte-americanas. (DONEDA, 2006, p. 264).

Entretanto, o papel dos Estados Unidos nesta conjuntura ainda demonstra timidez, considerando que, ao passo em que se apresenta como a nação mais evoluída tecnologicamente, surge diversas denúncias sobre casos de violação da privacidade por parte do serviço secreto norte americano, atingindo, inclusive, presidentes de outras nações.

Tal dicotomia talvez possa justificar o porquê que não se vislumbra atualmente no direito americano nenhuma lei específica e abrangente destinada à proteção dos dados pessoais dos cidadãos, em seu contexto geral, mas sim, diversas leis isoladas.

Este caráter visivelmente fragmentado do modelo de proteção norte-americano inerente aos dados pessoais parece refletir uma situação difícil à compreensão do jurista integrante do sistema romano-germânico, como é o caso da Alemanha e do Brasil. Contudo, não seria adequado se entender que esta fragmentação sinalizaria a ausência de um sistema voltado também à proteção dos dados pessoais.

Neste sentido, como bem pontuou Danilo Doneda (2006, p. 262), analisar a forma como vem se desenvolvendo a tutela da privacidade no ordenamento jurídico norte-americano "é tarefa que se impõe por uma série de motivos, ligados basicamente ao tráfego internacional

de dados pessoais e também ao poder de influência das escolhas do direito norte-americano em áreas na quais a tecnologia assume relevo".

Desta forma, no que se refere à proteção da privacidade e ao direito à informação, a *common law* norte americana contempla basicamente três normas jurídicas fundamentais, quais sejam: a *Freedom of Information Act* (FOIA) de 1967, a *Fair Credit Reporting Act* criada em 1970 e a *Privacy Act* de 1974. Somam-se a estas, outras variadas normas setorizadas e pontuais.

4.4.3 O *Freedom of Information Act* – FOIA (1967)

Uma das primeiras tentativas do parlamento americano para a regulação do acesso à informação dos indivíduos surge com a vigência da *Freedom of Information Act* (FOIA), no ano de 1967. É uma medida legal que visa à garantia de um direito contra o arbítrio governamental, não incluído entes privados.

Esta lei forneceu ao público o direito de reivindicar o acesso aos seus registros constantes de qualquer agência federal. É muitas vezes descrito como a lei que mantém os cidadãos no conhecimento sobre o seu governo. As agências federais são obrigadas a divulgar qualquer informação solicitada pela FOIA, exceto quando o interesse envolver questões de privacidade pessoal, de segurança nacional e de aplicação da lei.

Têmis Limberger (2007, p. 82) nos evidencia que a motivação para o surgimento deste diploma legal se deu pelo fato da grande preocupação da sociedade americana da época com o excessivo controle do governo sobre seus dados pessoais, bem como o gerenciamento de quase a metade dos dados informatizados do mundo.

O *Freedom of Information Act* (FOIA) se destina especificamente à regulação do acesso à informação. Ele visa assegurar aos cidadãos, às corporações e a outras entidades, o acesso às suas informações registradas em agências federais, contemplando o direito de obtenção de cópias destas mesmas informações. (DONEDA, 2006, p. 296-297).

O FOIA passou por alteração em 1986, quando fora promulgado o *Freedom of Information Reform Act*, cujo foco e preocupação relacionavam-se com a utilização da informação para fins de segurança pública. No ano de 1996 o Congresso Americano promulgou os *Freedom of Information Act Ammendments*, quando a nova fase da expansão

tecnológica já apresentava novos desafios diante da comunicação em rede. (DONEDA, 2006, p. 297).

Uma das características relevantes do FOIA são a fluidez, a simplicidade e a agilidade no seu procedimento. O cidadão, desconfiando de que suas informações estão sendo indevidamente manipuladas por agências governo, deverá, antes do requerimento, verificar se elas já não estão publicamente disponibilizadas, o que dispensaria a necessidade de se buscar a fonte, por óbvio, já identificada.

Em seguida, não tendo êxito nesta fase, poderá o cidadão requerer junto ao FOIA, por escrito, de forma razoável e fundamentada, os registros que procura. Um pedido ao FOIA pode ser feito para qualquer registro da agência e o cidadão tem a opção de receber as informações de forma impressa ou eletrônica.

Logo que recebida a solicitação do FOIA, a agência governamental inicia o processo de busca pelas informações e registros em resposta à solicitação do cidadão, quando então passa por uma triagem afim de que possam determinar quais e em que parte de cada, podem ser liberados.

A agência do governo redigirá ou apagará qualquer informação protegida de divulgação por uma das isenções da FOIA, a exemplo das questões de privacidade pessoal, de segurança nacional ou ainda de aplicação da lei. As demais informações, portanto, são enviadas ao cidadão, atendendo ao requerimento formulado via site (https://www.foia.gov/faq.html#processed).

4.4.4 O *Fair Credit Reporting Act* (1970)

O *Fair Credit Reporting Act*[8] (FCRA), promulgado em 1970, é mais um exemplo legal americano no sentido de direcionar esforços à proteção da privacidade e aos dados pessoais dos cidadãos e que, inclusive, serviu de referência à tutela do consumidor no direito brasileiro, ao positivar a Lei nº 8.078, de 1990.

Trata-se de um diploma que "aplica-se às empresas que emitem relatórios sobre os consumidores, em caso de análise de risco de crédito, assinatura de seguro e de contratação de empregados." (MENDES, 2014, p. 54). E a influência que exerceu sobre o direito brasileiro

[8] https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/fair-credit-reporting-act - acesso em: 05 jan. 2017.

encontra-se justamente na previsão do art. 43 e seguintes do Código de Defesa do Consumidor. (BRASIL, 2002).

O *Federal Fair Credit Reporting Act* (FCRA) busca promover a exatidão, a justiça e a privacidade das informações constantes nos arquivos de agências de gerenciam os bancos de dados sobre os consumidores, buscando impedir a manipulação e a divulgação indevida de informações que vão proporcionar danos reais aos cidadãos.

Entretanto, existem muitos tipos de agências de gerenciam relatórios de consumo, incluindo agências de crédito e agências especializadas, tais como aquelas que vendem informações sobre o histórico de cheques emitidos e compensados, dos registros médicos pretéritos para fins de avaliação de um seguro ou, ainda, de registros históricos sobre adimplência para a avaliação do risco em um novo contrato de locação.

O FCRA possibilitou se estabelecer obrigações de sigilo e a retificação dos dados financeiros de consumidores constantes dos bancos de dados geridos pelas operadoras de cadastros de crédito de consumo. Na previsão desta lei, as operadoras somente estarão obrigadas a revelar os dados armazenados na hipótese de cumprimento de ordem judicial, pelo consentimento expresso do interessado, ou, ainda, quando indícios apontem para que a informação será utilizada "para verificações concernentes a qualquer requisição do interessado de crédito, emprego, seguro, benefícios governamentais ou similares". (DONEDA, 2006, p. 294-295).

Em que pese esta lei tutelar um dos aspectos da proteção aos dados pessoais, não contempla uma série de outras demandas existentes, sobretudo porque a sua atuação é direcionada aos bancos de dados de consumo, não regulando em uma perspectiva mais abrangente toda a extensão do conteúdo dinâmico do *right to privacy*.

4.4.5 *Privacy Act* (1974)

Apesar da existência de algumas leis norte americanas que já regulam algum dos aspectos da privacidade, a *Privacy Act*[9], promulgado em 1974, pode ser considerada a primeira e a mais importante lei de proteção à privacidade, sobretudo pelo fato de ter estabelecido as bases para um direito geral da privacidade.

[9] https://www.gpo.gov/fdsys/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf - acesso em: 6 jan. 2017.

A expressão "*privacy"* abarca uma grande variedade de interesses que estão em permanente conflito com os demais meios de controle social dos cidadãos inseridos em uma sociedade da informação, cuja expansão tecnológica possibilita o surgimento de novas situações passíveis de violação da intimidade.

Dentre as previsões da *Privacy Act* está o reconhecimento de que a privacidade de um indivíduo é diretamente afetada pela coleta, manutenção, uso e disseminação das informações pessoais por parte das agências federais. Trata-se de uma das primeiras iniciativas legais de salvaguarda do direito à privacidade no contexto da proteção aos dados pessoais dos cidadãos. (PRIVACY ACT, 1974).

Apesar do pioneirismo desta lei, Têmis Limberger (2007, p. 82-83) chama a atenção para a crítica mais relevante que pode ser levantada contra ela, qual seja, o fato de possuir um conteúdo muito amplo e abranger apenas a proteção da privacidade do indivíduo quanto ao uso indevido dos registros por entidades e órgãos federais.

Entende Laura Mendes que a *Privacy Act* de 1974 de não se aplicaria apenas e tão somente à tutela da privacidade contra a atuação das agências governamentais federais, mas também, contra a conduta das empresas privadas que gerenciam e manipulam qualquer sistema de registro de dados pessoais para o governo. (MENDES, 2014, p. 54).

Entretanto, a *Privacy Act* não merece o descrédito apenas pelo fato de seu alcance se resumir à atuação das agências do governo, pois, uma justificativa plausível é que nos cadastro púbicos estão armazenados um grande número de informações sobre os cidadãos. Todavia, haveria de ter um instrumento legal igualmente eficaz na regulação dos dados pessoais manipulados por empresas privadas, garantindo também ao indivíduo o acesso aos registros que lhes dizem respeito. (LIMBERGER, 2007, p. 82-83).

A *Privacy Act* ainda reconhece que os desafios trazidos pela nova realidade tecnológica é um reflexo do uso crescente de computadores e da tecnologia de informação sofisticada, que, embora essencial para o funcionamento eficiente do governo, ampliou exponencialmente o dano à privacidade individual que pode ocorrer a partir de qualquer coleta, manutenção, uso ou disseminação de informações pessoais. (PRIVACY ACT, 1974)

De igual forma, já influenciada pela *Fair Credit Reporting Act* de 1970, a *Privacy Act* de 1974 ainda reconhece que as oportunidades para que um indivíduo obtenha um emprego, celebre um contrato de seguro ou de crédito, bem como outras proteções legais são ameaçadas

pelo uso indevido de certos sistemas de informação. Para tanto, a tutela destes interesses não pode ser negligenciada.

O consentimento do indivíduo assume um importante papel na *Privacy Act*, manifestando-se como um elemento central em torno do qual a lei se estrutura, haja vista prever que a eventual divulgação dos dados pessoais pelas agências governamentais exija o prévio consentimento do cidadão, sob pena de responsabilização civil e criminal dos envolvidos, em caso de violação.

A *Privacy Act* de 1974 apresenta, no entanto, diversos avanços significativos, sobretudo pelo fato de assegurar aos cidadãos o direito de acesso aos seus próprios dados pessoais armazenados em agências governamentais, bem como à garantia de retificação daqueles equivocados e, por fim, ao estabelecimento de regras definidas e circunstanciais para a divulgação destas informações pelo governo. (DONEDA, 2006, p. 295-296).

Entende Diógenes Ribeiro (2003, p. 40) que a proteção da privacidade no contexto da tradição norte-americana é enfatizada de forma extremamente acentuada quando comparada à experiência brasileira, pautada em instituições com um histórico democrático muito recente, somado ao desconhecimento da população em relação aos seus direitos.

4.4.6 Outras normas setorizadas de proteção à *privacy*, à informação e aos dados pessoais no direito nos EUA

No que tange à proteção da privacidade e ao direito à informação, a *common law* norte americana contempla basicamente três normas jurídicas fundamentais, quais sejam: a *Freedom of Information Act* (FOIA) de 1967, a *Fair Credit Reporting Act* criada em 1970 e a *Privacy Act* de 1974. Somam-se a estas, outras variadas normas setorizadas e pontuais.

No que se refere a estas normas setorizadas, são muito variadas e contemplam diversos outros aspectos da tutela da privacidade e dos dados pessoais dos indivíduos. Estas leis surgiram, dentre outros motivos, como consequência das discussões no Congresso e na sociedade, e que se relacionava com o projeto de criação do *National Data Center*.

Basicamente, se pretendia a criação de um grande banco de dados governamental alimentado com as informações dos cidadãos, o que possibilitaria o cruzamento destes dados para a descoberta de informações privadas que seriam armazenadas, possibilitando eventual

uso arbitrário e futuro pelo Estado, violando a prerrogativa última da liberdade dos cidadãos assegurada na Constituição Americana.

Um dos exemplos normativos esparsos é a *Family Educational Rights and Privacy Act*[10] (FERPA), promulgada em 1974, é uma lei federal que protege a privacidade dos registros de educação dos pais e alunos. A lei aplica-se a todas as escolas que recebem fundos sob um programa aplicável do Departamento de Educação dos Estados Unidos. Passou por emenda no ano de 2015, passando a proibir o financiamento de agências ou instituições educacionais que permitem a terceiros acessar os dados dos alunos.

O *Right to Financial Privacy Act*[11] (FPA) de 1978, tutela a privacidade financeira dos cidadãos, ao exigir que as agências governamentais notifiquem previamente o cidadão, para, querendo, se opor contra o ato de um banco ou de uma outra instituição de divulgar informações financeiras pessoais a uma agência estatal. A lei foi alterada nos últimos anos 1980 para permitir o adiamento da notificação em investigações sobre tráfico de drogas e espionagem.

O *Video Privacy Protection Act*[12] (VPPA) de 1988 é mais um dos exemplos. Fora criada para impedir a divulgação de dados e registros pessoais dos clientes constante dos bancos de dados das locadoras de filmes para videocassete ou material similar de áudio visual, sob pena de responsabilização em caso de violação.

Em relação ao *Driver's Privacy Protection Act*[13] (DPPA) de 1994, o mesmo visa assegurar a privacidade dos indivíduos ao impedir que qualquer funcionário do departamento estatal de trânsito revele as informações pessoais de terceiros, tais como o número da seguridade social, fotos, endereço, etc.

Existe ainda a *Gramm-Leach-Bliley Act*[14] (GLBA), promulgada em 1999, que oferece a proteção da privacidade e visa impedir a venda e o compartilhamento das informações financeiras dos indivíduos para entidades privadas, tais como os saldos bancários e os números de contas. Além disso, o GLBA codifica proteções contra *pretexting*, a prática de obter informações pessoais através de pretextos falsos.

[10] https://ed.gov/policy/gen/guid/fpco/ferpa/index.html - acesso em: 3 jan. 2017.
[11] http://www.accessreports.com/statutes/RFPA.htm - acesso em: 4 jan. 2017.
[12] http://www.accessreports.com/statutes/VIDEO1.htm - acesso em: 3 jan. 2017.
[13] http://www.accessreports.com/statutes/DPPA1.htm - acesso em: 3 jan. 2017.
[14] https://www.congress.gov/bill/106th-congress/senate-bill/900 - acesso em: 5 jan. 2017.

Há um exemplo muito recente no direto americano, a *Consumer Privacy Protection Act*[15] (CPPA) de 2015, que visa garantir a privacidade e a segurança de informações pessoais sensíveis, tais como o numero da seguridade social, os dados bancários, usuário e senha de uma conta de e-mail, nome e sobrenome, a localização geográfica e fotografias.

Este diploma tem ainda por objetivo prevenir e reduzir o roubo de identidade virtual, notificar violações de segurança envolvendo informações pessoais sensíveis e reforçar a assistência policial e outras proteções contra violações de segurança pela atuação de hackers, no acesso fraudulento e uso indevido de informações pessoais.

Podemos concluir que há uma abordagem diferente na comparação entre o modelo europeu de proteção aos dados pessoais e o norte-americano. O europeu se configura em uma base mais sistemática, preferindo a criação de leis gerais para a tutela da privacidade e dos dados pessoais em suas mais variadas perspectivas. No caso do direito americano, a tutela de mostra mais pragmática, favorecendo um cenário para o surgimento de diversas leis esparsas e pontuais sobre o assunto.

Entretanto, um fato histórico de grande relevância mundial marcou a sociedade americana, proporcionando um ambiente propício para uma mudança paulatina na extensão da tutela da privacidade nos Estados Unidos. Refere-se aqui ao atentado terrorista de 11 de setembro de 2011.

4.5 O 11 DE SETEMBRO DE 2011 E OS NOVOS DESAFIOS À GARANTIA DO *RIGHT TO PRIVACY* E DOS DADOS PESSOAIS NOS EUA

4.5.1 *USA Patriot Act* (2001) e o *USA Freedom Act* (2015)

Apesar do progresso que vinha demonstrando o congresso norte-americano no que se refere à proteção da privacidade e aos dados pessoais dos indivíduos, tal conjuntura passou a ser ameaçada, haja vista que, no dia 11 de setembro de 2011, fundamentalistas islâmicos vinculados à rede terrorista Al Qaeda, organizaram um grande atentado suicida contra a cidade de Nova Iorque, com a queda de quatro aviões em pontos estratégicos, matando milhares de pessoas.

[15] https://www.congress.gov/bill/114th-congress/senate-bill/1158/text - acesso em: 5 jan. 2017.

Este ataque evidenciou a fragilidade no sistema de segurança do governo americano, exigindo que o governo americano tomasse medidas à retomada da confiança internacional. Inicia-se a Guerra ao Terror, como um grande programa de governo, visando desarticular a rede terrorista através do combate em território Afegão.

Dentre as medidas de exceção adotadas pelos Estados Unidos após este fato, está o *USA Patriot Act*[16], um Decreto assinado pelo presidente George W. Bush, no Salão Leste da Casa Branca, no dia 26 de outubro de 2011, um mês depois dos atentados terroristas ocorridos em 11 de setembro do mesmo ano.

A prioridade do Departamento de Justiça era a de evitar futuros ataques terroristas. Desde os atentados de 11 de setembro de 2001, o *Patriot Act* tinha desempenhado um papel-chave no que tange à proteção dos americanos contra os planos terroristas dedicados a destruir a América.

Dentre as medidas autorizadas por esta lei estão a realização de vigilância eletrônica para investigar supostos crimes terroristas, incluindo a adoção de escutas telefônicas. Neste sentido, o governo americano passou a interceptador todos os dados e registros pessoais possíveis na internet, para, em prol da segurança nacional, devassar a privacidade das pessoas sob o pretexto de uma guerra contra o terrorismo.

Stefano Rodotá chama a atenção para o fato de que, mesmo antes do 11 de setembro, as estratégias de mercado e a expansão dos bancos de dados já apontavam indícios para o que se chamava de o "fim da privacidade". Entretanto, após os atentados terroristas de 2001, "a privacidade na era do terror" parece estar sendo condenada. Deixou de ser vista como um direito fundamental, passando a ser compreendida como um obstáculo à segurança, sendo superada por legislações emergenciais. (RODOTÁ, 2008, p.13-4)

O autor ainda identificou três motivos básicos para justificar o distanciamento entre a realidade e a garantia de um direito fundamental: o primeiro consiste no fato de que, após o 11 de setembro, muitas das garantias individuais foram reduzidas em todo o mundo, a exemplo do próprio *Patriot Act*, nos EUA. (RODOTÁ, 2008, p. 14).

O segundo motivo seria que a redução das garantias atingiu, inclusive, o mundo dos negócios, que também passaram a ter suas transações monitoradas pelo governo a fim de estancar eventual financiamento aos extremistas. E o terceiro e último motivo diz respeito ao fato de que o momento de exceção possibilita o desenvolvimento de novas oportunidades

[16] https://www.justice.gov/archive/ll/highlights.htm - acesso em: 5 jan. 2017.

tecnológicas, que passaram a estar disponíveis para o monitoramento da vida privada das pessoas. (RODOTÁ, 2008, p. 14).

Conclui o autor que este retrato social traduz a realidade de que os cidadãos são "cada vez mais transparentes e que os órgãos públicos estão mais e mais fora de qualquer controle, político e legal. Isto implica uma nova distribuição de poderes políticos e sociais." (RODOTÁ, 2008, p. 15).

O *USA Patriot Act* fora perdendo eficácia com o decorrer dos anos, quando diversas das suas disposições expiraram, sobretudo pela troca de governantes americanos, tendo a figura de Barack Obama, um perfil político de cunho mais moderado.

Em 2 de junho de 2015, o Congresso Norte-Americano promulga o *USA Freedom Act*[17], que restaurou grande parte das disposições da lei patriótica, porém de forma modificada e adaptada à realidade atual.

O *USA Freedom Act* impõe alguns novos limites para a coleta em massa dos chamados "metadados" de telecomunicações de cidadãos norte-americanos por agências de inteligência americanas, incluindo a Agência de Segurança Nacional.

Fora uma medida de resposta contra o período anterior de excessiva violação à privacidade sob o pretexto da "segurança nacional". Um dos exemplos é o caso da denúncia feita por Edward Snowden (HARDING, 2014), que revelou o grande esquema de espionagem realizado pelo governo norte-americano contra indivíduos em todo o planeta, incluindo cidadãos americanos, coletando e manipulando os dados e as comunicações pessoais até mesmo dos presidentes e chefes de Estado de diversos países, tais como a Alemanha, o México e o Brasil.

[17] https://www.congress.gov/114/plaws/publ23/PLAW-114publ23.pdf - acesso em: 6 jan. 2017.

5 A TUTELA DOS DADOS PESSOAIS NO DIREITO BRASILEIRO

5.1 A PROTEÇÃO AOS DADOS PESSOAIS COMO UM DIREITO FUNDAMENTAL

Todo indivíduo necessita de uma seara de proteção da sua intimidade e da sua vida privada, de modo que possa desenvolver as capacidades físicas e psíquicas que o possibilitem desenvolver a sua autonomia em sociedade. E desta forma, o objeto dos direitos da personalidade não é exterior ao sujeito de direito, ao contrário de outros bens jurídicos tutelados pelo ordenamento de uma nação.

Os dados pessoais de um indivíduo se caracterizam por refletir os pressupostos mais íntimos da sua privacidade, necessários ao pleno desenvolvimento dos direitos da personalidade. Neste sentido, trata-se de um direito fundamental e inerente à dignidade humana.

No contexto brasileiro, a privacidade fora assegurada através da disposição do artigo 5º, inciso X da Constituição Federal de 1988, que, de forma expressa, prevê a inviolabilidade aos direitos da personalidade, tais como, 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.

Ao prever expressamente a intimidade e a vida privada como interesses tutelados pela sociedade brasileira, a Carta Magna deixou clara a importância dada pelo legislador originário no que tange à garantia deste direito, ao incluí-lo no rol seleto dos direitos fundamentais, exigindo o reconhecimento enquanto normas dotadas do atributo da obrigatoriedade.

Conforme Dirley da Cunha Júnior, todas as normas integrantes de Constituições rígidas, independente do conteúdo que carregam, teriam uma estrutura e natureza inerentes à normas jurídicas, dotadas de juridicidade, imperatividade e obrigatoriedade. (CUNHA JÚNIOR, 2014, p. 32).

Acrescenta que a Constituição, além de imperativa, é suprema quando comparada às demais normas do ordenamento jurídico, exigindo observância e compatibilidade seja quanto ao modo de elaboração (conformação formal), seja pela matéria tratada (conformação material). (CUNHA JÚNIOR, 2014, p. 32).

Em havendo o reconhecimento do direito à privacidade a partir do próprio texto constitucional, se conclui que a proteção aos dados pessoais do indivíduo é uma derivação da tutela da privacidade, porém não se limita a esta, e é também um pressuposto para o desenvolvimento da personalidade. Assegurar o sigilo dos dados pessoais é reconhecer a própria tutela da privacidade.

Neste sentido, conforme o entendimento de Danilo Doneda, "a proteção de dados pessoais no ordenamento brasileiro não se estrutura a partir de um complexo normativo unitário, mas em uma série de disposições cujo propósito e alcance nos são fornecidos pela leitura da cláusula geral da personalidade." (DONEDA, 2006, p. 323).

O direito brasileiro vem se desenvolvendo de forma muito tímida no que se refere à tutela dos dados pessoais, ao contrário do que já vinha ocorrendo na Europa e nos Estados Unidos desde a década de 70, onde já apresentavam normas legais específicas com o objetivo de regular a coleta, a transformação e a distribuição das informações de cunho privado.

Justificando a proteção aos dados pessoais como um direito fundamental, Laura Mendes (2014, p. 173) destaca que a Constituição Federal de 1988 passou a adotar dois mecanismos importantes para a tutela deste direito, quais sejam, "o direito material à proteção de dados pessoais", baseado no artigo 5º, X, da Carta Magna e, ainda, "a garantia instrumental para a proteção deste direito", através da previsão da ação de *habeas data* no artigo 5º, inciso LXXII.

Além do texto constitucional, verifica-se também a proteção aos direitos da personalidade nos artigos 11 e seguintes do Código Civil (2002). Por fim, são tutelados alguns aspectos da proteção aos dados pessoais no Código de Defesa do Consumidor (CDC), sobretudo no que tange às regras de gestão dos bancos de dados de consumo.

Esta realidade fragmentada não satisfaz, na integralidade, todas as exigências que a tutela do sigilo aos dados pessoais dos indivíduos pode requerer. Apesar do direito brasileiro situar-se dentro da tradição romano-germânica, cuja tutela da informação já integra uma lei geral, parece que o mesmo vem se assemelhando à forma americana, também pulverizada em diversas leis setorizadas tutelando algum dos aspectos da proteção da privacidade.

Apesar de grande parte de a doutrina brasileira defender a possibilidade de extensão da titularidade dos direitos da personalidade às pessoas jurídicas, e, de igual forma, a tutela da privacidade, entendemos, assim como Anderson Schreiber, que existiria uma impossibilidade manifesta. Segundo o autor:

> Os direitos da personalidade gravitam em torno da condição humana, e, por isso mesmo, não tem qualquer relação com as pessoas jurídicas. As sociedades, as associações, as fundações e todas as demais espécies de entes abstratos detêm a personalidade em sentido subjetivo, ou seja, possuem aptidão para a aquisição de direitos e obrigações. Não gozam, apesar disso, da especial proteção que o ordenamento jurídico reserva ao núcleo essencial da condição humana. (SCHREIBER, 2013, p. 21-22).

Em se tratando a esfera da intimidade e do segredo prerrogativas defendidas pela ordem constitucional por refletirem na dignidade do indivíduo, de certo, tais garantias não podem ser estendidas à iniciativa privada. A ressalva necessária é que apenas alguns dos atributos da personalidade, como o nome, podem ser estendidos às pessoas jurídicas, resguardando o núcleo essencial da condição humana às pessoas naturais.

Não é demais salientar que, com a expansão da sociedade da informação, o indivíduo assume a sua personalidade perante um novo espaço social: o digital. Trata-se de uma arena onde as pessoas assumem perfis que geram um imenso fluxo de informações e dados através do acesso a sítios na internet e troca de mensagens entre usuários em uma rede aberta onde muitos podem ter acesso a ela.

Os dados pessoais gerados com a navegação na internet dos cidadãos brasileiros são armazenados e geridos pelo Estado e por empresas privadas, que os mantém em grandes bancos de dados que se mostram capazes de cruzar as informações para descobrir os padrões de comportamento dos indivíduos, o que tornará possível traçar perfis para tomada futura de decisões, boas ou ruins.

A omissão do ordenamento jurídico brasileiro em regulamentar a tutela dos dados pessoais, manifesta uma situação extremamente temerária ao indivíduo, por possibilitar que suas informações mais íntimas sejam coletadas, armazenadas e eventualmente utilizadas, violando a prerrogativa da dignidade da pessoa humana.

Em contrapartida, surgem no direito brasileiro, os primeiros indícios de que a proteção aos dados pessoais vem se transformando em um interesse relevante para a sociedade. O advento do CDC ampliou a possibilidade de tutela, contudo, fora com a promulgação da Lei nº 12.965 de 23 de abril de 2014, também conhecida como o “Marco Civil da Internet”, que o tema vem sendo enfrentado de forma mais clara, embora ainda pendente de maior aprofundamento.

5.2 A PREVISÃO DO *HABEAS DATA* NO DIREITO BRASILEIRO

A Constituição Federal de 1988, no seu artigo 5º, inciso LXXII, previu expressamente um instrumento de garantia para a proteção de alguns dos aspectos da tutela da privacidade e dos dados pessoais: o *habeas data*. O instituto visa assegurar tanto o conhecimento acerca das informações referentes ao próprio interessado que o solicita quanto a correção de inconsistências ou equívocos constantes destes arquivos. (EFING, 2002, p. 65).

Trata-se de um remédio heroico de grande relevância para o ordenamento jurídico brasileiro, equiparando-o às garantias previstas no direito comparado. O direito à privacidade não poderia ser devidamente assegurado "se não houvesse a criação de instrumentos jurisdicionais devidamente adaptados a darem efetividade aos direitos materialmente assegurados" (BASTOS; MARTINS, 1999, p. 253).

Neste sentido, a mera previsão do direito à privacidade e, consequentemente, da proteção aos dados pessoais no ordenamento brasileiro, desacompanhada de instrumentos jurídicos específicos para a sua garantia revelar-se-ia ineficaz, comprometendo a própria validade e o respeito à Constituição. (BASTOS; MARTINS, 1999, p. 254).

De acordo com Renato Afonso Gonçalves, o *habeas data* pode então ser entendido como um "resultado da necessidade que modernamente se apresentou de proteção do individuo contra o poder, cada vez mais dilatado, do Estado e de instituições privadas, de armazenarem informações sobre as pessoas, e com base nelas operarem em detrimento da privacidade e da liberdade dos indivíduos". (GONÇALVES, 2003, p. 103).

O *habeas data* fora regulamentado através da Lei nº 9.507, de 12 de novembro de 1997, que passou a dispor acerca do direito de acesso à informação e, ainda, sobre a ritualística processual do remédio constitucional. (BRASIL, 2012a). Conforme o artigo 2º desta lei, o interessado deverá protocolar o requerimento no sentido de obter, junto ao órgão ou entidade depositária dos dados, a correção ou anotação destas informações. Trata-se do procedimento pré-judicial do *habeas data*, cuja resposta deverá ocorrer em 48 (quarenta e oito) horas. (Art. 2º, *caput*).

O interesse de agir para a impetração judicial do *habeas data* surge apenas quando o interessado não vislumbra êxito na tentativa extrajudicial de obter as informações junto ao gestor do banco de dados, bem como quando se depara com um óbice à retificação daquelas informações inconsistentes e equivocadas. (BUENO, 2012, p. 76).

Este também é o teor pacificado pela jurisprudência nacional, através da Súmula nº 02 do Superior Tribunal de Justiça (STJ), quando prevê que "não cabe o *habeas data* (CF 5º, LXXII, letra 'a') se não houver a recusa de informações por parte da autoridade administrativa". (SÚMULA nº 2 STJ).

Em que pese a norma regulamentadora nada prever acerca de quem poderá ser autor ou o réu no procedimento judicial do *habeas data*, o entendimento imediato é no sentido de que "pode impetrar *habeas data* todo aquele que pretende tutelar os bens materiais descritos no art. 7º, I a III, da Lei nº 9.507/97, inclusive pessoas jurídicas." (BUENO, 2012, p. 80).

No que se refere àquele contra quem é dirigido o *habeas data*, a previsão do artigo 7º esclarece que o destinatário passivo será aquele que detém a informação passível de correção, sendo irrelevante se o mesmo possui natureza pública ou privada. Segundo Bueno, o "caráter público do bem, pois, é reconhecido em função de seu objeto, não em razão da pessoa que o presta". (BUENO, 2012, p. 81).

Neste contexto, tanto as instituições financeiras, quanto os bancos oficiais, os bancos particulares, as empresas da seara imobiliária, bem como aquelas inerentes ao ramo comercial, industrial ou de prestação de serviços, uma vez atuando como gestoras de bancos de dados, são consideradas destinatárias passivas do *habeas data*. (WAMBIER, 1991, p. 116).

O comum no que tange aos bancos de dados de consumo é a divulgação do histórico econômico do consumidor, certificando ou não a sua idoneidade financeira para futuras transações comerciais. Neste sentido, somente quando se manifestar uma conduta positiva do indivíduo no mercado de consumo é que tais informações poderão ser armazenadas, quando então se tornarão passíveis de correção acerca daqueles dados inconsistentes. (BESSA, 2011, p. 201). A partir daí tornar-se-á possível o manejo do *habeas data*.

5.3 A PROTEÇÃO AOS DADOS PESSOAIS NO CÓDIGO DE DEFESA DO CONSUMIDOR

Na sociedade atual, o mercado de consumo compõe a vida cotidiana das sociedades de forma inegável, onde as relações contratuais gradativamente vão se tornando cada vez mais complexas, exigindo que o Direito acompanhe esta realidade e disponibilize ferramentas para a regulação dos conflitos evidenciados, restabelecendo a harmonia social.

Diante desta conjuntura, a primeira norma jurídica em vigor no direito brasileiro a tratar expressamente acerca de algum dos aspectos do direito à privacidade e da proteção aos dados pessoais, inclusive disciplinando o funcionamento de novas tecnologias de processamento de dados, fora a Lei nº 8.078 de 1990, conhecida como o Código de Defesa do Consumidor (CDC). (BRASIL, 1990).

Trata-se uma norma de vanguarda, com elevado conteúdo principiológico e destinada à proteção do consumidor, parte hipossuficiente da relação contratual, contra os abusos praticados pelos fornecedores de um produto ou serviço.

A proteção aos dados pessoais é objeto de tutela no artigo 43 do CDC, onde disciplina a existência dos bancos de dados e dos cadastros de dados dos consumidores. A redação do *caput* lhe assegura o acesso às informações existentes em cadastros, fichas, registros e dados pessoais, inclusive as informações de consumo que são armazenadas a seu respeito.

Os bancos de dados constituem um aglomerado de dados e informações estruturadas logicamente e que podem ser geridas com ou sem o manejo da informática. (DONEDA, 2006, p. 157). Entretanto, a sociedade da informação proporcionou o aprimoramento desta ferramenta, que passou a se utilizar de alta capacidade de armazenamento.

Neste sentido acrescenta Danilo Doneda:

> O banco de dados informatizado, produto da tecnologia aplicada ao tratamento de informações pessoais, apresenta um potencial superior: ele pode armazenar um grande volume de informações, processá-las rapidamente, agregá-las e combiná-las em uma multiplicidade de modos em tempo irrisório se comparado com idêntica operação realizada em um banco de dados de tratado manualmente (2006, p. 158-159).

Segundo Antônio Carlos Efing, os bancos de dados de consumo são “sistemas para coleta aleatória de informações, normalmente arquivadas sem requerimento do consumidor, que dispõem de organização mediata, a atender necessidades latentes através de divulgação permanente de dados obrigatoriamente objetivos exclusivamente econômicos”. (EFING, 2002, p. 35).

Em verdade, o CDC não veda o funcionamento dos referidos cadastros e bancos de dados com informações dos consumidores, entretanto, exige o atendimento aos requisitos legais, que tem por objetivo restabelecer o equilíbrio entre as partes e proteger a seara íntima da parte hipossuficiente, que não possui recursos para se empoderar em face à dinâmica agressiva do mercado.

Uma das estratégias potencialmente lesivas aos interesses dos cidadãos é a má utilização dos bancos de dados com o objetivo de rotular o indivíduo conforme seu histórico de adimplência em contratos anteriores. No caso brasileiro, instituições tais como o SPC e o Serasa atuam na gestão destes tipos de cadastros de restrição ao crédito.

Constatando-se uma situação de inadimplência em face de algum credor legalmente constituído, os dados do consumidor e da transação são repassados pelo interessado às instituições de proteção ao crédito, a fim de que se restrinja o acesso futuro do devedor a uma nova oportunidade de crédito, enquanto não saldada a dívida original. São também denominados como bancos de dados de proteção ao crédito. (BESSA, 2011, p. 23).

Ocorre que esta situação apresenta um grande potencial de violação à privacidade, sobretudo pela possibilidade de manejo inapropriado e abusivo dos dados pessoais dos cidadãos, nascendo daí a necessidade de regulação pelo ordenamento brasileiro, o que ocorreu por meio do artigo 43 e seguintes do Código de Defesa do Consumidor.

De certo, em nossa sociedade atual pautada na expansão tecnológica e nas regras do mercado, o consumidor não sobrevive sem o crédito. Neste sentido, ter um histórico creditício pretérito e atual de status positivo é um patrimônio de extrema valia para o desenvolvimento da dignidade do indivíduo, sobretudo quando pretende se adquirir produtos e serviços ou, ainda, buscar uma ocupação profissional.

Neste sentido, não se pode perder de vista que os bancos de dados de consumo e os cadastros de crédito exercem grande influência sobre o modo de vida dos indivíduos, o que evidencia uma realidade onde este sequer possui o efetivo controle sobre as informações pessoais que são coletadas, geridas e compartilhadas por terceiros.

A norma consumerista prevista no seu artigo 43 e seguintes fora inspirada no *Fair Credit Reporting Act* (FCRA) do direito norte americano, promulgada em 1970. Trata-se de um diploma que "aplica-se às empresas que emitem relatórios sobre os consumidores, em caso de análise de risco de crédito, assinatura de seguro e de contratação de empregados." (MENDES, 2014, p. 54).

É considerada a primeira lei norte-americana destinada à tutela do *right to privacy*, vinculando-a com os casos de informações armazenadas em banco de dados, justamente por se dispor a regular escritórios de proteção ao crédito e cadastros de consumidores. (DONEDA, 2006, p. 141).

O objetivo do *Federal Fair Credit Reporting Act* (FCRA) é o de promover a exatidão, a justiça e a privacidade das informações constantes nos arquivos de agências de gerenciam os bancos de dados sobre os consumidores, buscando impedir a manipulação e a divulgação indevida de informações que vão proporcionar danos reais aos cidadãos.

De igual forma ocorreu com o CDC. Segundo os parágrafos 1º ao 6º do artigo 43, os bancos de dados destinados ao armazenamento de informações dos cidadãos devem ser claros, objetivos e com conteúdo verídico, inclusive contendo linguagem de fácil compreensão. O cadastro não poderá ser mantido por prazo superior a cinco anos. (ARRUDA ALVIM, 1997).

Não é outro o posicionamento de Antônio Herman Benjamin, quando descreve as peculiaridades na atuação destes órgãos:

> nesses organismos que cadastram devedores (SPCs, Serasa e congêneres), onde qualquer registro, mesmo os mais inofensivos, transmuda-se de imediato em informação capaz de 'impedir ou dificultar novo acesso ao crédito junto aos fornecedores', a regra é a da destruição total do assento, uma vez pago o débito ou verificado um dos impedimentos temporais. (BENJAMIN, 1999, p. 389).

O registro dos dados dos consumidores junto aos cadastros de crédito somente pode ser inserido mediante prévia comunicação por escrito ao devedor a fim de que possa tomar ciência do fato e, querendo, possa purgar a mora. De igual forma, ao consumidor é assegurado o direito de retificação dos dados cadastrados quando constatada a inexatidão, devendo o fornecedor de produtos e serviços proceder à correção no prazo de cinco dias. (CDC, art. 43).

Uma ressalta fundamental constante do § 5º do artigo 43 do CDC está no fato de se garantir uma prescrição quanto ao prazo de permanência junto a estes bandos de dados de crédito. Segundo a norma citada, uma vez consumada a prescrição quinquenal relativa à cobrança de débitos do consumidor, não mais poderão ser fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam dificultar ou impedir o acesso do consumidor a um novo crédito futuro junto aos fornecedores. (BRASIL, 1990).

A coleta e a manipulação de dados pessoais dos cidadãos e o consequente armazenamento das informações em bancos de dados de alto desempenho, levantam uma grande discussão pelo fato de estarem sob a posse de empresas privadas. Não há garantia de que estas pessoas jurídicas não compartilharão com terceiros as informações retidas.

De igual forma, também não há garantias de que o mercado não possa criar bancos de informações ocultas ao controle estatal, com o objetivo de estruturar um perfil de consumo

dos indivíduos que poderá ser comercializado e consultado secretamente pelos fornecedores, violando a privacidade dos dados pessoais armazenados.

Esta problemática evidencia a grande complexidade que envolve os casos onde se relatam danos aos indivíduos pelo mau uso dos dados pessoais, sobretudo pela empresa que gerencia os cadastros de informações sobre o crédito. (COVIZZI, 2000, p. 35).

Em uma sentença proferida pela 16ª Vara Cível de Porto Alegre[18], nos autos de uma Ação Coletiva envolvendo o Ministério Público e a Confederação Nacional de Dirigentes Lojistas, se considerou que a atividade de comercialização de informações cadastrais dos consumidores por parte do SPC Brasil seria ilícita, haja vista que desconsiderou a exigência de anuência prévia dos interessados.

Na referida ação, o Ministério Público constatou que os órgãos de proteção ao crédito vendiam os dados e as informações coletadas pelos consumidores através de seu sítio destinado às empresas, objetivando a promoção de ações de marketing e telemarketing, a exemplo das malas diretas, venda de listas de contatos telefônicos e outras comunicações que ofereciam produtos e serviços.

Os dados pessoais compartilhados envolviam o nome completo, o telefone, o domicílio, numeração dos documentos pessoais, a data de nascimento, o nome dos genitores, o contato de e-mail, dentre outras tantas informações pessoais protegidas pelo sigilo.

Não é demais ponderar que, diante da complexidade e da inovação da temática na sociedade atual, as questões suscitadas devem ser balizadas considerando uma harmonia entre as previsões do Código de Defesa do Consumidor, da Lei do Cadastro Positivo (Lei nº 14/2011) e, ainda, respeitando o Marco Civil da Internet (Lei nº 12.965/2014), haja vista que tal comercialização de informações tem como cenário principal a Internet.

5.4 A LEI DO CADASTRO POSITIVO Nº 12.414/2011

Em complementação às previsões do artigo 43 do Código de Defesa do Consumidor, surge no ordenamento jurídico brasileiro a Lei nº 12.414 de 2011, também conhecida como a Lei do Cadastro Positivo.

[18] 16ª Vara Cível de Porto Alegre. Processo n. 001/1.14.0178998-7. Ministério Público x Confederação Nacional de Dirigentes Lojistas. Juiz Sílvio Tadeu de Ávila. J. Em 28 de Agosto de 2015.

Sancionada em 9 de junho de 2011, a Lei do Cadastro Positivo busca estabelecer as regras para a formação e a consulta aos bancos de dados com informações de adimplemento seja de pessoas físicas ou jurídicas, com o objetivo de formar um histórico de crédito. Para além a simples coleta das informações básicas referentes à inadimplência, uma série de outros registros serão armazenados pelo fornecedor de modo a evidenciar o nível de pontualidade dos pagamentos em relação a um histórico pretérito. (BESSA, 2011, p. 60).

Desta forma, não há impedimento para que um histórico de adimplência anterior seja cruzado com aquele outro destinado às informações negativas, quando então as informações de cunho positivo poderão mostrar-se mais desfavoráveis quando somadas a um historio de inadimplência contumaz. (COSTA, 2012, p. 25).

Uma informação negativa é aquela que não favorece a concessão do crédito ao consumidor, por conta de históricos pretéritos que aumentam o risco do fornecedor, que então recusa o contrato. (BESSA, 2001, p. 34). Para Eduardo Arruda Alvim, as informações negativas são aquelas que são "verdadeiras, mas que não recomendam o consumidor conquanto bom cumpridor de contratos". (ARRUDA ALVIM, 1997, p. 172). Já no entendimento exposto por Fábio Ulhôa Coelho, esta informação de cunho negativo seria "aquela que, de qualquer modo, influi ou pode influir depreciativamente na formação da imagem do consumidor perante o fornecedor". (COELHO, 1999, p. 219). São aqueles que "desabonam o interessado, ainda que verdadeiras". Atuam como "obstáculos a novas relações de consumo ou a circunstâncias que acarretam dificuldade de crédito". (GUERREIRO, 1993, p. 98).

A Lei do Cadastro Positivo deixa claro logo no parágrafo único do artigo 1º, que os bancos de dados instituídos ou mantidos por pessoas jurídicas de direito público interno serão regidos por legislação específica. Ou seja, a Lei nº 12.414/2011 destina-se apenas à regulação das práticas realizadas pela iniciativa privada, não atingindo bancos de dados alheios aos interesses do consumo.

De acordo com o parágrafo 3º do artigo 3º, são vedadas as práticas envolvendo as anotações de informações excessivas, tais como aquelas que não estiverem vinculadas à análise de risco de crédito ao consumidor. De igual forma, seguindo a mesma previsão da Lei Portuguesa n° 67 de 1998, também fora proibida a manutenção dos dados sensíveis, aqueles inerentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas.

De acordo com Laura Schertel Mendes:

> a categoria dos dados sensíveis está relacionada à percepção de que o armazenamento, o processamento e a circulação de alguns tipos de dados podem se constituir em um risco maior à personalidade individual, especialmente se utilizados com intuito discriminatório. Os dados referentes a raça, opção sexual, saúde e religião são exemplos desse tipo. (2014, p. 74).

Outro não é o entendimento exposto por Danilo Doneda, quando reconhece que os dados sensíveis são um produto da realidade prática da tutela dos dados pessoais e que não poderia ser desconsiderada, haja vista que não se pode negar que exista uma diferença entre "o efeito do tratamento destes dados em relação aos demais". (DONEDA, 2006, p. 161).

A Lei nº 12.414/2011, no seu artigo 4º, ainda prevê que a eventual abertura de cadastros de dados predispõe a autorização prévia do potencial cadastrado mediante consentimento informado do consumidor, na mesma forma como prevista no artigo 6º da Diretiva Europeia 97/66/CE (1997), seja através da sua assinatura exarada em um instrumento específico, seja por meio de uma cláusula apartada.

Dentre os direitos dos consumidores especificados nesta lei (artigo 5º) estão a prerrogativa de obter o cancelamento do cadastro quando solicitado, acessar gratuitamente as informações sobre ele existentes no banco de dados, bem como a de impugnar qualquer informação sobre ele erroneamente anotada em banco de dados. Neste sentido, deve o fornecedor comunicar estas alterações a todos àqueles com os quais compartilhou a informação do consumidor.

De igual forma, seguindo a mesma previsão que já constava na Diretiva Europeia e também no artigo 10 da Lei Portuguesa n° 67 de 1998, a Lei Brasileira do Cadastro Positivo garantiu o direito do consumidor de ser previamente informado sobre o armazenamento, a identidade do gestor do banco de dados, o objetivo do tratamento dos dados pessoais e os destinatários para os quais os dados foram compartilhados.

Contemplando o princípio da finalidade ou da destinação específica da coleta, o referido diploma também passou a consignar o direito do consumidor de ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados. Na hipótese de alteração do propósito original, o usuário deverá ser cientificado afim de que possa manifestar sua concordância, se assim o desejar.

A Lei nº 12.414/2011 não fora omissa quanto à responsabilidade daquele que compartilha os dados pessoais a terceiros. Conforme a disposição do seu artigo 9º, somente é permitido o compartilhamento das informações acerca do adimplemento do consumidor quando expressamente autorizado pelo mesmo, seja por meio da assinatura aposta em um instrumento contratual específico ou através de uma cláusula apartada.

Por conseguinte, o diploma legal ainda assegura no seu § 1º do mesmo artigo 9º que, aquele que receber os dados pessoais dos consumidores através do compartilhamento equipara-se, para todos os fins legais, àquele que originariamente os transmitiu, assumindo a responsabilidade solidária por todos os eventuais prejuízos que possam ter causado ao consumidor por conta da exposição indevida das informações que estão sob a sua posse.

Em que pese o grande avanço trazido pela vigência da Lei do Cadastro Positivo, no sentido de buscar assegurar a privacidade dos consumidores, no ano de 2014 surge uma norma legal de extrema relevância neste contexto, qual seja, a Lei nº 12.965 de 2014, conhecida como o Marco Civil da Internet.

5.5 O MARCO CIVIL DA INTERNET E A TUTELA DOS DADOS PESSOAIS

Mesmo após um longo processo de defasagem normativa que durou cerca de 40 (quarenta) anos desde as primeiras normas de proteção aos dados pessoais surgidas na Europa, o Brasil, enfim, sanciona a Lei nº 12.965 no dia 23 de abril de 2014, popularmente conhecida como o Marco Civil da Internet.

Quando ainda era um projeto de lei, o tema vinha sendo objeto de exaustivos debates nas duas Casas do Congresso Nacional durante alguns anos, sem que se chegasse a um consenso. Contudo, em 2013 surge a divulgação de provas de um grande esquema de espionagem cibernética operacionalizado pela agência de segurança norte-americana contra diversas nações mundiais e chefes de Estado, inclusive do Brasil, o que fez com que a temática ganhasse ares de maior seriedade.

A pressão popular gerada, aliada à situação constrangedora do governo brasileiro quanto ao fato, evidenciaram a sua completa fragilidade em assegurar a sua soberania, muito menos garantir a proteção cibernética dos cidadãos brasileiros usuários da rede. Esta conjuntura fez com que o projeto assumisse a prioridade de tramitação nas Casas Legislativas,

enfrentando novos debates e discussões, quando, enfim, fora aprovado e posteriormente sancionado em abril de 2014.

Desta forma, o Marco Civil da Internet busca demonstrar o seu objetivo fundamental no sentido de proporcionar a esperada segurança jurídica a todo cidadão e usuário da internet no Brasil, elencando princípios, garantias, direitos e deveres para a tutela da liberdade, bem como as diretrizes que deverão orientar a atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

A Lei nº 12.965/14, já no seu artigo 2º, reconheceu expressamente o potencial da escala mundial inerente à internet, evidenciando que deixou de considerá-la um mero espaço de entretenimento, mas sim, uma arena de desenvolvimento da personalidade do indivíduo e para o exercício pleno da cidadania.

Neste sentido, buscou elencar diretrizes que reconhecem a pluralidade e a diversidade dos usuários, bem como a finalidade social da rede, não deixando de evidenciar que a livre iniciativa, a livre concorrência e a defesa dos interesses dos consumidores, permanecem em posição de destaque no ordenamento jurídico brasileiro.

Dentre os pontos fundamentais trazidos pelo Marco Civil da Internet está o rol de princípios estruturais que orientam a atuação do poder público, dos entes privados e dos usuários em rede. Buscou-se no artigo 3º reafirmar a garantia da liberdade de expressão, da comunicação e da manifestação do pensamento, acrescentando, inclusive, expressamente, a proteção da privacidade.

A segurança do cidadão também fora incluída entre os princípios fundamentais previstos na Lei nº 12.965/2014, de acordo com os meios técnicos compatíveis com a padronização internacional. Por conseguinte, manifestou a preocupação com a responsabilização dos agentes de acordo com suas atividades, embora tal previsão ainda penda de regulamentação específica.

Dentre os direitos e garantias dos usuários previstos no artigo 7º, está a inviolabilidade da intimidade e da vida privada das pessoas, bem como do sigilo quanto ao fluxo de suas comunicações pela internet, inclusive, disponibilizando todo o arcabouço da responsabilidade civil para reparação indenizatória na hipótese de violação.

De igual forma, vedou-se expressamente o compartilhamento dos dados pessoais dos usuários a terceiros, inclusive dos registros de conexão e de acesso a aplicações de internet,

salvo mediante consentimento livre, expresso e informado do usuário, adequando-se ao que dispõe as normas de origem europeia inerentes à temática.

No artigo 10 fora disciplinada a proteção aos registros, aos dados pessoais e às conexões privadas de acesso à internet, cuja previsão assegurou, ao menos no plano teórico, a preservação da intimidade e da vida privada dos cidadãos envolvidos. Por conseguinte, atribuiu ao provedor responsável pela guarda dos dados e registros a obrigação de garantir estas previsões, exceto mediante requisição judicial.

Outra questão relevante também fora disposta na lei do Marco Civil da Internet e gira em torno das condições de armazenamento dos dados pessoais por parte dos provedores de aplicações. De acordo com os artigos 13 a 15, estas pessoas jurídicas têm o dever de manter os dados e registros de acesso a aplicações de internet sob sigilo, ao menos por um ano, podendo ser estendido a pedido da autoridade competente.

Não se pode negar que o Marco Civil da Internet possibilitou uma maior proteção ao usuário da rede no Brasil. Entretanto, para que esta norma legal possa atingir seu pleno alcance, exigia-se a regulamentação de diversas das suas disposições, o que somente fora proposta através do Decreto nº 8.771/2016, que será melhor referido no item seguinte.

Ocorre que a solução do problema parece ultrapassar o campo de atuação da norma legal, exigindo uma solução mais ampla e conjunta. E neste sentido pontua Eduardo Tomasevicius Filho:

> É aspecto intrigante do Marco Civil da Internet a ingenuidade do legislador brasileiro de manter a pretensão de solução de problema de escala mundial, com efeitos extraterritoriais, por meio de uma lei nacional. A própria estrutura da internet permite que as violações dos direitos das pessoas ocorram em qualquer parte do mundo, passando ao largo da jurisdição brasileira. (TOMASEVICIUS FILHO, 2016, p. 276-277).

A Lei nº 12.965/2014 definiu como seu objetivo fundamental proporcionar segurança jurídica a todo cidadão e usuário da internet no Brasil, elencando princípios, garantias, direitos e deveres para a tutela da liberdade, bem como as diretrizes que deverão orientar a atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

Entretanto, um dos grandes desafios enfrentados pelo governo brasileiro é a realidade de que a quase totalidade dos provedores de conexão em funcionamento no território nacional não possuem representação jurídica no Brasil, embora gerenciem vultosos bancos de dados com informações de cidadãos nacionais, impossibilitando a submissão dos mesmos às normas

jurídicas internas. O simples fato de um sítio utilizar o idioma português não o obrigada a esta sujeição.

Também não fora objeto de previsão na Lei nº 12.965/2014 como será operacionalizada e mensurada a apuração das infrações na hipótese de distribuição não autorizada dos dados pessoais dos indivíduos entre provedores de conteúdo e de conexão.

Apesar destas e outras críticas que poderiam ser levantadas, é possível destacar alguns pontos positivos no que se refere à iniciativa de sancionar o Marco Civil da Internet no Brasil. Um dos avanços diz respeito à vedação ao uso de técnicas para a censura, o bloqueio, o monitoramento ou a análise dos dados que circulam pela internet, quando em território nacional. (TOMASEVICIUS FILHO, 2016, p. 278).

Outro ponto positivo seria a forma como a lei nº 12.965/2014 buscou regular as hipóteses autorizadas para uso dos *cookies*, pequenos ficheiros depositados no computador do internauta pelos sítios visitados. O artigo 7º, inciso VIII passou a exigir o prévio consentimento do usuário, o que se manifestou como um grande avanço contra esta ferramenta indesejada de coleta de informações. (TOMASEVICIUS FILHO, 2016, p. 278).

Não se poderia deixar de mencionar a previsão da Lei nº 12.965/2014 no que tange à responsabilidade do provedor de conexão da internet em relação aos danos eventualmente identificados aos indivíduos através dos conteúdos gerados por terceiros na rede. Segundo a previsão dos artigos 18 e 19, o provedor estará isento da responsabilidade civil nestes casos, salvo se, instado por ordem judicial específica à retirada do conteúdo, recusar-se ao cumprimento do comando.

Em que pese a tentativa louvável do Poder Legislativo brasileiro no sentido de sancionar o Marco Civil da Internet, diversas das suas previsões pendiam de regulamentação, impossibilitando a satisfação efetiva do direito fundamental à proteção aos dados pessoais, ao menos até o ano de 2016, quando fora promulgado o Decreto nº 8.771/16.

5.6 UMA TENTATIVA DE REGULAMENTAÇÃO DO MARCO CIVIL DA INTERNET ATRAVÉS DO DECRETO Nº 8.771/2016

No dia 11 de maio de 2016 fora sancionado pelo governo brasileiro o Decreto nº 8.771, que regulamentou o Marco Civil da Internet, dispondo sobre algumas temáticas e, entre

elas, encontra-se a indicação quanto aos procedimentos de guarda e proteção de dados pelos provedores de conexão e de aplicações, ao tempo em que também indicar as medidas de transparência na requisição de dados cadastrais pela administração pública. (BRASIL, 2016)

Em relação especificamente à tutela dos dados pessoais, o Decreto supracitado estabelece que as autoridades administrativas legalmente autorizadas por lei para a requisição das informações dos usuários aos provedores de internet, deverão explicitar o fundamento legal que o habilita ao acesso das informações, bem como a motivação para o requerimento. (art. 11, caput).

Neste sentido, a requisição por autoridades administrativas dos dados cadastrais de usuários da Internet exigem prévia autorização legal, na hipótese, por exemplo, da necessidade de colheita de provas para investigação de ilícitos penais, tais como os crimes de lavagem ou ocultação de bens, direitos e valores (art. 17-B da Lei nº 9.613/98) e os referentes à organização criminosa (art. 15 da Lei nº 12.850/13).

Evidencia ainda o Decreto nº 8.771/16 que os pedidos de acesso devem discriminar precisamente os indivíduos objetos da consulta, não sendo permitido pedido coletivo ou genérico (art. 11, § 3º). Ademais, prevê ainda a norma que a Administração Pública Federal, por meio da autoridade responsável, se compromete a divulgar em seu sítio oficial, anualmente, um relatório contendo estatísticas acerca das requisições dos dados pessoais cadastrados. (art. 12).

O decreto regulamentador também passou a prever diretrizes sobre padrões de segurança na atuação dos provedores de conexão de internet, no que se refere à guarda, ao armazenamento e ao tratamento de dados pessoais e das comunicações privadas (art. 13, I a IV):

> 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. (BRASIL, 2016).

Percebe-se a preocupação do legislador para com o controle do acesso aos dados pessoais dos indivíduos, estabelecendo uma rígida ritualística aos provedores de conexão afim de que seja possível identificar a origem da distribuição indevida, a exemplo do uso da autenticação de acesso aos registros, da criação de um inventário detalhado dos acessos e, ainda, da utilização de ferramentas como a encriptação.

Um ponto de grande relevância trazido com Decreto nº 8.771/16 diz respeito a um conceito para a expressão "dados pessoais". Segundo a norma, o dado é uma informação relacionada "à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa". (art. 14, I)

O artigo 17 da norma regulamentadora atribui a responsabilidade pela regulação, fiscalização e apuração das infrações ao Decreto à Anatel (art. 17), nos termos da Lei nº 9.472, de 16 de julho de 1997, bem como à Secretaria Nacional do Consumidor, no que tange à fiscalização e apuração das infrações. (art. 18)

Apesar das intenções de vanguarda do referido decreto, a implementação destas medidas ensejam um custo que nem sempre é considerado pelo legislador, bem como parece não se ter a completa noção dos custos com a fiscalização. Diante de uma realidade de recursos escassos[19], cabe ao poder público tomar uma decisão alocativa (AMARAL, 2001, p. 37), de modo a priorizar os interesses sociais relevantes, estando dentre eles, a proteção da privacidade no meio digital.

Não se pode ainda traçar uma estatística sobre o cumprimento desta norma. O tema é muito recente e passou à pauta secundária diante da crise política e econômica enfrentada pelo país. Entretanto, o futuro é desafiador, mesmo com a vigência deste Decreto. A dinâmica social é bastante ampla e complexa para ser solucionada através de uma legislação nacional, desconsiderando um arranjo internacional mais eficaz.

[19] No mesmo sentido é o pensamento de Stephen Holmes e Cass Sunstein: "[…] *the cost of rights is in the first instance a descriptive, not a moral, theme. […] True, the cost of rights can be morally relevant, for a theory of rights that never descends from the heights of morality into the world of scarce resources will be sorely incomplete, even from a moral perspective. […] they cannot fully explore the moral dimensions of rights protection if they fail to consider the question of distributive justice".* (HOLMES; SUNSTEIN, 2000, p. 18-19).

6 CONSIDERAÇÕES FINAIS

Chega-se à conclusão de que todo indivíduo necessita da proteção de uma seara última da sua intimidade e da sua vida privada, de modo que possa desenvolver as capacidades físicas e psíquicas que o possibilitem adquirir a sua autonomia em sociedade. E desta forma, quando se refere aos direitos da personalidade, em verdade contempla um catálogo de garantias fundamentais que são inerentes ao indivíduo e que contemplam os aspectos mais reservados da sua existência em sociedade, apresentando uma íntima correlação com a tutela da privacidade.

O fomento dos direitos da personalidade perpassa pelo respeito à privacidade, em uma perspectiva mais ampla do que apenas uma tutela negativa de ser deixado em paz. A sociedade da informação e do consumo proporciona uma nova realidade tecnológica que, apesar de trazerem avanços, também carrega consigo novas situações de violação da vida privada, tais como a coleta, o tratamento e o compartilhamento indevidos dos dados pessoais dos indivíduos, sobretudo no meio digital.

Não restam dúvidas de que tal circunstância ameaça os interesses dos cidadãos e do próprio Estado. A ausência de regulamentação quanto à coleta e o tratamento dos dados pessoais, ou a sua disposição insuficiente, tanto pode favorecer o seu uso como uma ferramenta totalitária por parte dos governos, quanto pode ser manejada pela iniciativa privada no intuito de padronizar e classificar os indivíduos em prol do estrito consumo.

Este novo direito fundamental à proteção dos dados pessoais já vem sendo paulatinamente reconhecido no direito comparado, a exemplo do que vem ocorrendo no continente europeu e nos Estados Unidos, fruto da preocupação com o dano em potencial que a exposição das informações pessoais pode causar aos direitos e garantias fundamentais dos indivíduos. O direito brasileiro já vem acompanhando este movimento.

Com o surgimento da Lei nº 12.965/14, o Brasil sanciona sua primeira norma legal destinada à proteção dos direitos dos usuários da rede mundial de computadores, que fora regulamentada por meio do Decreto nº 8.771/16, estabelecendo diretrizes sobre padrões de segurança na atuação dos provedores de conexão de internet.

Não se pode deixar de reconhecer a tentativa louvável do Brasil no sentido de proteger este novo direito fundamental, estruturado a partir das necessidades da sociedade moderna. Entretanto, também não se pode desconsiderar que a dinâmica complexa da sociedade da informação exige um aperfeiçoamento constante dos institutos legais, de modo a acompanhar as mudanças sociais.

O surgimento de uma norma legal não induz, necessariamente, à sua plena efetivação. Os diplomas vigentes no direito brasileiro parecem não serem suficientes para se atribuir ao indivíduo o controle sobre os seus próprios dados pessoais, sobretudo porque a internet é uma tecnologia transnacional. Em tais normas não parece ter sido considerada as limitações territoriais, o custo inerente à implementação das ferramentas de segurança e, tampouco, a estrutura necessária para a fiscalização destas normas.

O tema é muito recente no Brasil e passou a ser considerado como uma pauta secundária diante da grave crise política e econômica enfrentada pelo país. Entretanto, as violações à intimidade ainda remanescem e o futuro é desafiador, mesmo com a vigência do Decreto regulamentador. A dinâmica social é bastante ampla e complexa para ser solucionada através de uma legislação nacional. Uma solução mais eficaz parece emergir para além das fronteiras do Estado, através de arranjos internacionais mais eficazes que vinculem o maior número possível de nações, o que melhor se compatibilizaria com o caráter transnacional da internet.

A doutrina nacional também precisa assumir seu papel na difusão deste conhecimento. É importante um esforço pela consolidação de uma dogmática onde se possam construir reflexões que fundamentarão uma base sólida para auxiliar o Poder Judiciário na aplicação atual e futura deste direito, bem como orientar a atuação do Estado em prol da implementação de políticas públicas eficazes neste sentido.

O papel da sociedade civil também é fundamental neste processo. É importante que a difusão deste conhecimento possa favorecer o empoderamento dos cidadãos acerca dos riscos à privacidade identificados a partir desta nova realidade tecnológica, garantindo-lhe o desenvolvimento das prerrogativas inerentes aos seus direitos da personalidade, fomentando a sua autonomia enquanto sujeito de direitos.

REFERÊNCIAS

ALEXY, Robert. *Teoria dos Direitos Fundamentais*. Trad. Virgílio Afonso da Silva. 2. ed. São Paulo: Malheiros, 2012.

AMARAL, Gustavo. *Direito, Escassez & Escolha*: em busca de critérios jurídicos para lidar com a escassez de recursos e as decisões trágicas. São Paulo: Renovar, 2001.

ARRUDA ALVIM, Eduardo. *Código do Consumidor Comentado*. 4. ed. São Paulo: RT, 1997.

BASTOS, Celso Ribeiro; MARTINS, Ives Gandra. *Comentários à Constituição Federal de 1988*. São Paulo: Saraiva, 1999.

BAUDRILLARD, Jean. *La Sociedad de Consumo*. Sus mitos, sus estructuras. Traducción de Alcira Bixio. España: Siglo, 2007.

BAUMANN, Zygmunt. *Vida Para Consumo*. A transformação das pessoas em mercadoria. Tradução Carlos Alberto Medeiros. Rio de Janeiro: Jorge Zahar, 2008.

BELLEIL, Arnaud. *@ Privacidade*. Portugal: Instituto Piaget, 2002.

BENJAMIN, Antônio Herman Vasconcelos. *Código de Defesa do Consumidor comentado pelos autores do anteprojeto*. 6. ed. Rio de Janeiro: Forense Universitária, 1999.

BESSA, Leonardo Roscoe. *Cadastro positivo*: comentários à Lei 12.414, de 9 de junho de 2011. São Paulo: Revista dos Tribunais, 2011.

BÍBLIA Sagrada: Antigo e Novo Testamento. Gênesis. Traduzida em português por João Ferreira de Almeida. 2. ed. rev. e atual. São Paulo: Sociedade Bíblica do Brasil, 1993. Parte I.

BITTAR, Carlos A. *Os direitos da personalidade*. 3. ed. São Paulo: Forense Universitária, 1999.

BRASIL. Conselho da Justiça Federal. Enunciado 4 da I Jornada de Direito Civil. Disponível em: <http://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/i-jornada-de-direito-civil.pdf/view>. Acesso em: 10 set. 2016.

BRASIL. Conselho da Justiça Federal. Enunciado 275 da IV Jornada de Direito Civil. Disponível em: <http://www.cjf.jus.br/cjf/CEJ-Coedi/jornadas-cej/IV%20JORNADA%20E%0DIREITO%20CIVIL%202013%20ENUNCIADOS%20APROVADOS.pdf/view>. Acesso em: 10 set. 2016.

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil*. Brasília, DF, Senado, 1998.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor. Dispõe sobre a proteção do consumidor e dá outras providências. *Diário Oficial [da] República Federativa do Brasil*, Brasília, DF, 12 set. 1990. Seção 1, suplemento, p. 1.

BRASIL. Lei nº 10.406, de 10 de Janeiro de 2002. Institui o Código Civil. *Diário Oficial [da] República Federativa do Brasil*, Brasília, DF, 11 jan. 2002. Seção 1, p. 1.

BRASIL. Lei nº 12.414, de 9 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. *Diário Oficial [da] República Federativa do Brasil,* Brasília, DF, 10 jun. 2011. Seção 1, p. 2.

BRASIL. Conselho da Justiça Federal. *Jornadas de direito civil I, III, IV e V*: enunciados aprovados. Brasília, DF: Centro de Estudos Judiciários, 2012.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal e dá outras providências. *Diário Oficial [da] República Federativa do Brasil,* Brasília, DF, 3 dez. 2012a. Seção 1, p. 1.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial [da] República Federativa do Brasil,* Poder Executivo, Brasília, DF, de 24 abr. 2014. Seção 1, p. 1.

BRASIL. Decreto nº 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. *Diário Oficial [da] República Federativa do Brasil,* Poder Executivo, Brasília, DF, de 11 maio 2016. Seção 1, edição extra, p. 7.

BUENO, Cassio Scarpinella. *Habeas Data*. In: DIDIER JR., Fredie (Org.). *Ações Constitucionais*. 6. ed. Salvador: JusPodivm, 2012.

CASTELLS, Manuel. *A era da informação*: economia, sociedade e cultura. A sociedade em rede. São Paulo: Paz e Terra, 1999. v. 1.

COELHO, Fábio Ulhôa. *Comentários ao Código de Proteção ao Consumidor*. São Paulo: Saraiva, 1999.

COHEN, Jean. *Sociedade civil e globalização*: repensando categorias. *Dados: Revista de Ciências Sociais*, Rio de Janeiro, v. 46, n. 3, p. 419-459, 2003.

COMPARATO, Fábio Konder. *A Afirmação Histórica dos Direitos Humanos*. 7.ed. rev. e atual. São Paulo: Saraiva, 2010.

COMUNIDADE EUROPEIA. Directiva 95/46 CE do Parlamento Europeu e do Conselho. Jornal Oficial das Comunidades Européias, n. L 281/31, 23 nov. 1995. Disponível em: < http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_pt.pdf >. Acesso em: 01 fev. 2017.

COUNCIL OF EUROPA. *European Treaty Series* –n.108. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. Strasbourg, 28 jan. 1981. Disponível em: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayCTMontent?documentId=0900001680078b37>. Acesso em: 6 jan. 2017.

COSTA, Carlos Celso Orcesi da. *Cadastro Positivo - Lei n. 12.414/2011*: comentada artigo por artigo. São Paulo: Saraiva, 2012.

COSTA JR, Paulo José. *O direito de estar só*. São Paulo: Revista dos Tribunais, 1995.

COVIZZI, Carlos Adroaldo Ramos. *Práticas abusivas da SERASA e do SPC*: Doutrina, legislação jurisprudência. 2. ed. São Paulo: Edipro, 2000.

CUNHA JÚNIOR, Dirley da. *Controle de Constitucionalidade*. Teoria e Prática. 7. ed. Salvador: JusPodivm, 2014.

CUPIS, Adriano de. *Os direitos da personalidade*. Tradução Afonso Celso Furtado Rezende. 2. ed. São Paulo: Quorum, 2008.

DAVID, René. *Os Grandes Sistemas do Direito Contemporâneo*. Tradução Hermínio A. Carvalho. 4. ed. São Paulo: Martins Fontes, 2002.

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

EFING, Antônio Carlos. *Banco de Dados e Cadastro de Consumidores*. São Paulo: RT, 2002.

EUROPA. *European Union website*. Diretiva 97/66/CE. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002L0058&from=en. Acesso em: 5 jan. 2017.

EUROPA. *European Union website*. Diretiva 2002/58/EG. Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002L0058&from=en. Acesso em: 5 jan. 2017.

EUROPA. *European Union website*. Diretiva 2009/136/EG. Disponível em: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF. Acesso em: 2 jan. 2017.

GIDDENS, Anthony. *O mundo na era da globalização*. Tradução Saul Barata. Lisboa: Editorial Presença, 2000.

GONÇALVES, Carlos Roberto. *Direito Civil Brasileiro.* 10. ed. São Paulo: Saraiva, 2012. v. 1.

GONÇALVES, Renato Afonso. *Bancos de dados nas relações de consumo*. São Paulo: Max Limonad, 2003.

GUERREIRO, José Alexandre Tavares. *Comentários ao Código do Consumidor*. Rio de Janeiro: Forense, 1993.

HARDING, Luke. *Os Arquivos Snowden*. A História Secreta do Homem mais Procurado do Mundo. Trad. Bruno Correia e Alice Klesck. São Paulo: LeYa, 2014.

HOLMES, Stephen; SUNSTEIN, Cass. *The Cost of Rights*: Why Liberty Depends on Taxes. New York: W. W. Norton & Company, 2000.

JENNINGS, Charles; FENA, Lori. *Priv@cidade.com*: como preservar sua intimidade na era da internet. São Paulo: Futura, 2000.

KANT, Immanuel. *Fundamentação da Metafísica dos Costumes*. São Paulo: Abril Cultural, 1980. p. 103-162.

KOATZ, Rafael Lorenzo-Fernandez. *As Liberdades de Expressão e de Imprensa na Jurisprudência do STF*. In: SARMENTO, Daniel; SARLET, Ingo Wolfgang (orgs.). Direitos

Fundamentais no Supremo Tribunal Federal: Balanço e Crítica. Rio de Janeiro: Lúmen Júris, 2011.

LIMBERGER, Têmis. *O direito à intimidade na era da informática*: *a necessidade de proteção de dados pessoais*. Porto Alegre: Livraria do Advogado, 2007.

MANSO, Eduardo Vieira. *A informática e os direitos intelectuais*. São Paulo: RT, 1995.

MARTÍNEZ, Gregorio Peces-Barba. *La dignidade de la persona desde la filosofia del derecho*, 2. ed. Madrid: Dykinson, 2003.

MAYER-SCHÖNBERGER, Viktor. *Generational development of data protection in Europe*. In: AGRE, Philip E.; ROTENBERG, Marc. (Ed.). *Technology and privacy:* the new landscape. Cambridge: Mit Press, 2001.

MENDES, Laura Schertel. *Privacidade, Proteção de Dados e Defesa do Consumidor*. Linhas gerais de um novo direito fundamental. Rio de Janeiro: Saraiva, 2014.

NISSENBAUM, H. *Privacy in Context:* Technology, Policy, and the Integrity of Social Life. Palo Alto, CA: Stanford University Press, 2010.

OCDE. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. 2002. Disponível em: <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotection ofprivacyandtransborderflowsofpersonaldata.htm - acesso em: 10/01/2017.

RIBEIRO, Diógenes V. H. *Proteção da Privacidade*. Rio Grande do Sul: Unisinos, 2003.

RODOTÁ, Stefano. *A vida na sociedade de vigilância:* a privacidade hoje. Rio de Janeiro: Renovar, 2008.

SARLET, Ingo Wolfgang. *Dignidade da Pessoa Humana e Direitos Fundamentais na Constituição de 1988*. 9. ed. rev. e atual. Porto Alegre: Livraria do Advogado, 2012.

SAUNDERS, Anthony. *Medindo o risco de crédito*: novas abordagens para o *value at risk* e outros paradigmas. Rio de Janeiro: Qualitymark, 2000.

SCHREIBER, Anderson. *Direitos da personalidade*. 2. ed. rev. e atual. São Paulo: Atlas, 2013.

SILVA, José Afonso da. *Curso de Direito Constitucional Positivo*. 10. ed. São Paulo: Malheiros, 1996.

SOARES, Guido Fernando Silva. *Common Law:* Introdução ao Direito dos EUA. 2. ed. São Paulo: Revista dos Tribunais, 2000.

SOARES, Ricardo Maurício Freire. *O Princípio Constitucional da Dignidade da Pessoa Humana*. São Paulo: Saraiva, 2010.

SOUZA, Ródnei Bernardino. *O modelo de collection scorinq como ferramenta para a gestão estratégica do risco de crédito*. 2000. 75 p. Dissertação (MBA) - Curso de Pós Graduação da EAESP/FGV, São Paulo, 2000.

TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. *Estudos Avançados*, São Paulo, v. 30, n. 86, jan./abr. 2016.

WACKS, Raymond. *Personal Information:* Privacy and the Law. Oxford: Clarendon Press, 1989.

WALDROM, Jeremy. Dignity and Rank: in memory of Gregory Vlastos (1907–1991). *European Journal Sociology*, Cambridge, v. 48, n. 2, p. 201-237, aug. 2007.

WAMBIER, Luiz Rodrigues. *Tutela jurisdicional das liberdades públicas*. Curitiba: Juruá, 1991.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. *Harvard Law Review*, Cambridge, v. 4, n. 5, Dec. 1890. Disponível em: <http://faculty.uml.edu/gallagher/randeisprivacy.htm>. Acesso em: 26 out. 2016.