A tutela da privacidade na Sociedade da Informação

A proteção dos dados pessoais no Brasil

Joana de Moraes Souza Machado

Fi

A sociedade contemporânea é marcada pelos avanços ocorridos na tecnologia de comunicação, possibilitando a socialização das informações, que passaram a ter um papel fundamental na vida das pessoas, considerando-se a sua visibilidade pela sociedade pós-industrial. No entanto, tal evolução acabou por invadir o cotidiano das pessoas e empresas, transformando inclusive, as formas de relacionamento. A vida dos indivíduos passou a ficar mais exposta, o que culminou com sérios perigos à sua privacidade e intimidade. Nesse contexto, não poderia mais se compreender a privacidade apenas pelo aspecto do isolamento e recato. A privacidade passou a ser entendida também como direito à autodeterminação informativa. Todos os indivíduos devem ter o controle das informações acerca de si. O grande problema dessa temática foi justamente a verificação da inexistência absoluta de controle por parte do seu titular. Soma-se a isso o fato de que até 2018 não havia no Brasil uma lei de proteção de dados pessoais, dificultando assim o controle destes dados. Esta obra tem como objetivo apresentar argumentos criteriosamente sistematizados que sustentem a efetiva tutela da pessoa, em frente ao tratamento de dados pessoais por agentes privados. Foi demonstrada neste estudo, a premente necessidade de controle das informações pessoais, o qual só se mostrará viável com o advento de uma legislação protetiva destes dados, que seja adequada à realidade do nosso país. Para alcançar os objetivos propostos, foi utilizada a técnica da pesquisa bibliográfica, com uso de doutrinas e jurisprudências nacionais e alienígenas. Utilizou-se ainda a pesquisa documental, valendo-se de materiais que não receberam tratamento analítico, como artigos científicos, reportagens de revistas e documentos internacionais de proteção de dados pessoais.

9 788556 964946

editora fi.org

CC BY SA

A Tutela da Privacidade na Sociedade da Informação

Direção Editorial

Lucas Fontella Margoni

Comitê Científico

Prof.ª Dr.ª Joyceane Bezerra de Menezes
Universidade de Fortaleza – UNIFOR

Prof. Dr. Eduardo Rocha Dias
Universidade de Fortaleza – UNIFOR

Prof. Dr. Francisco Luciano Lima Rodrigues
Universidade Federal do Ceará - UFC

Prof.ª Dr.ª Marcia Correia Chagas
Universidade Federal do Ceará - UFC

Prof. Dr. Regnoberto Marques de Melo Junior
Universidade Federal do Ceará - UFC

A Tutela da Privacidade na Sociedade da Informação

A proteção dos dados pessoais no Brasil

Joana de Moraes Souza Machado

Diagramação: Marcelo A. S. Alves
Capa: Lucas Margoni

O padrão ortográfico e o sistema de citações e referências bibliográficas são prerrogativas de cada autor. Da mesma forma, o conteúdo de cada capítulo é de inteira e exclusiva responsabilidade de seu respectivo autor.

Todos os livros publicados pela Editora Fi
estão sob os direitos da Creative Commons 4.0
https://creativecommons.org/licenses/by/4.0/deed.pt_BR

http://www.abecbrasil.org.br

Dados Internacionais de Catalogação na Publicação (CIP)

MACHADO, Joana de Moraes Souza

A tutela da privacidade na sociedade da informação: a proteção dos dados pessoais no Brasil [recurso eletrônico] / Joana de Moraes Souza Machado -- Porto Alegre, RS: Editora Fi, 2018.

230 p.

ISBN - 978-85-5696-494-6

Disponível em: http://www.editorafi.org

1. Direito à privacidade. 2. Direitos fundamentais. 3. Dados pessoais. 4. Sociedade da informação.; I. Título.

CDD: 340

Índices para catálogo sistemático:
1. Direito 340

Sumário

1 17
A tutela da personalidade e a expansão do conceito de privacidade
1.1 A evolução histórica do direito da personalidade e a cláusula geral de tutela da pessoa. 18
1.2 A personalidade como valor e as situações jurídicas existenciais 31
1.3 A tutela da privacidade e sua correlação com a estrutura da propriedade 38
1.4 O mundo tecnológico e o conceito contemporâneo de privacidade 46

2 69
A tutela da privacidade e a informação
2.1 A evolução conceitual do direito à privacidade 70
2.2 A cumplicidade entre privacidade e intimidade 86
2.3 A relação entre privacidade e informação 93
2.4 Cogência da cessão da informação e a necessidade de proteção. 110

3 117
A proteção internacional dos dados pessoais
3.1 Considerações acerca dos dados pessoais 117
3.2 A proteção de dados pessoais na União Europeia 123
3.2.1 Desenvolvimento do modelo europeu 128
3.3 O modelo norte-americano de proteção de dados pessoais 153

4 167
O controle de dados pessoais no direito brasileiro
4.1 A proteção constitucional e infraconstitucional de dados pessoais no Brasil 168
4.2 O *Habeas Data* no direito brasileiro 173
4.2.1 O Habeas Data em outros países da América Latina 183
4.3 A importância do Marco Civil da Internet para proteção de dados pessoais 186
4.4 Lei de proteção de dados pessoais no Brasil 192
4.4.1 O consentimento no tratamento de dados pessoais 199
4.4.2 A Autoridade Nacional de proteção de dados pessoais 207

Conclusão 217

Referências 221

Introdução

A globalização e os avanços tecnológicos nas áreas da informação e da comunicação trouxeram muitos impactos para a vida social, econômica e política das pessoas. Possibilitou o acesso mais rápido às informações e a sua socialização. Estas, por sua vez, assumem um importante papel na consolidação de várias situações jurídicas que emergem no contexto da sociedade pós-industrial.

O uso da *internet* e a rapidez da comunicação são características marcantes desta sociedade, também chamada sociedade da informação. Não obstante as novas dimensões, a coleta e o tratamento de informações pessoais alcançaram um patamar potencialmente nocivo à privacidade.

A evolução tecnológica acabou por invadir o cotidiano das pessoas e das empresas, transformando até mesmo as formas de relacionamento. Sem muitas vezes considerar os riscos à privacidade e à intimidade, as pessoas estão expostas a uma visibilidade permanente.

Tradicionalmente as violações à privacidade eram entendidas de uma forma particular, analisando-se apenas os aspectos do recato e do sossego. Coube ao célebre ensaio *The right to privacy,* de Warren e Brandeis, em 1890, estabelecer os primeiros contornos do que se tutelaria como privacidade. Atualmente, o conceito se ampliou para permitir o enfrentamento das lesões e ameaças suscitadas na era digital.

A privacidade, como direito fundamental e da personalidade traduz uma garantia essencial ao pleno desenvolvimento do indivíduo e ao exercício das chamadas liberdades públicas, tendo como expressão a dignidade da pessoa humana.

O debate acerca da privacidade não se restringe mais ao tema clássico da defesa da esfera privada contra as invasões externas. Outras fontes de ameaça e lesão podem comprometer a privacidade que também passa a ser considerada como o direito que tem a pessoa de controlar a circulação e tratamento das informações pessoais.

Faz-se necessário se rediscutir os mecanismos de tutela da privacidade a fim de expandi-los para fazer face às demandas da sociedade da informação. Entende-se que os instrumentos tradicionais, emergentes do paradigma liberal burguês são insuficientes. Nos dias atuais, a privacidade escapa àquela conceituação tradicional, albergada no direito de estar só ou à proteção da vida privada familiar. Hoje, deve ser tutelada como direito à autodeterminação informativa. O indivíduo deve exercer o controle sobre a coleta e tratamento dos dados ao seu respeito, considerando que são integrantes da sua própria personalidade.

A informação passou a ter um papel fundamental na sociedade globalizada e a sua circulação se mostra como indispensável tanto para o poder público, quanto para as empresas privadas. Por intermédio da avaliação de dados, o Estado determinará a política pública adequada ao seu país. Para as organizações privadas, a informação pode ser um bem valioso para se estabelecerem as modalidades de *marketing* e publicidade com o fim de atrair clientes.

Todavia, torna-se cada vez mais difícil identificar os tipos de informação acerca dos quais o cidadão estaria disposto a divulgar completamente. O indivíduo acaba renunciando definitivamente ao controle das modalidades de seu tratamento e as atividades dos sujeitos que as utilizam. Percebe-se que até as informações mais banais podem, se integradas a outras, provocar danos à pessoa.

Nesse contexto, os cidadãos têm o direito de exercer um controle direto sobre as informações fornecidas, atribuindo-lhes uma espécie de poder. Entretanto, raramente o cidadão perceberá o sentido que a coleta de dados pode assumir numa organização

complexa e dotada de meios sofisticados para o seu tratamento, podendo escapar do risco da utilização destas informações por parte de agentes privados.

A problemática fundamental deste trabalho enfoca exatamente a ausência de conhecimento e de controle do titular sobre a coleta, armazenamento e tratamento dos seus dados pessoais por parte das empresas públicas e privadas. Busca-se investigar, neste estudo se, atualmente, os instrumentos legais disponíveis acerca da proteção de dados pessoais são adequados e suficientes, considerando o estágio atual da tecnologia.

A relação entre o indivíduo isolado e as grandes organizações de coleta de dados é absolutamente assimétrica. Faz com que o controle pareça algo ilusório. Dessa forma, mostra-se o presente trabalho relevante do ponto de vista social, considerando que as pessoas precisam ter consciência de que as informações que a elas dizem respeito fazem parte da personalidade e, por esta razão necessitam de controle por parte de seus titulares.

O objetivo-fim deste trabalho é apresentar argumentos criteriosamente sistematizados que sustentem o agenciamento da efetiva tutela da pessoa em frente ao tratamento de informações pessoais constantes de bancos de dados. Será realizado um estudo analítico reflexivo do direito à privacidade, qualificando-o como direito fundamental e da personalidade que se espraia para além do conceito tradicional de ascendência liberal burguês. Ao mesmo tempo, analisar-se-á a necessidade de controle das informações pessoais por parte dos seus titulares.

Nesse sentido, argumenta-se: seria de fato necessária a regulamentação por legislação específica de proteção de dados pessoais, considerando as leis já existentes em matéria de proteção da intimidade e da vida privada? Nos dias atuais, os instrumentos colocados à disposição do cidadão são suficientes e adequados para uma efetiva tutela dos dados pessoais?

Para enfrentar estas questões, a Europa elaborou uma série de leis, que merecem ser lembradas. A Organização para

Cooperação e Desenvolvimento Econômico (OCDE), em 1980, adotou os Princípios Diretrizes para a proteção de dados pessoais, abrangendo todas as formas utilizadas para processamento automatizado de informações pessoais. A Convenção 108, do Conselho da Europa, reconhecendo a importância de se conciliarem os valores fundamentais do respeito à privacidade e à livre circulação de informações, elaborou uma legislação baseada em princípios, como os da finalidade, necessidade e publicidade.

A União Europeia, em 1995, enfrentou tais problemas, usando como marco fundamental a proteção da dignidade da pessoa humana como princípio e demais subprincípios. A Diretiva 95/46/CE do Parlamento Europeu e do Conselho da União Europeia trata da proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Este documento determinou que os diversos países elaborassem princípios e regras para a proteção dos dados pessoais. Posteriormente, foi elaborada a Carta de Direitos Fundamentais, em 2000, reconhecendo a proteção de dados pessoais como direito autônomo.

Mais recentemente, foi aprovado o Regulamento Geral de Proteção de Dados Pessoais na Europa, denominado Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. Tal regulamento revoga a Directiva 95/46/CE, que por muitos anos regulou a matéria da proteção de dados na Europa, bem como orientou diversas legislações no mundo.

Nesse sentido, percebe-se que a tutela dos dados pessoais na Europa é realizada por uma série de legislações baseadas em princípios, fazendo-se concluir que a privacidade nos dias de hoje é mais bem tutelada na Europa, do que nos EUA, de onde foi importada.

No Brasil, até 2018 não havia legislação específica de proteção dos dados pessoais. Foi aprovada recentemente a Lei Geral de Proteção de Dados Pessoais – Lei 13.709/18. Havia tão somente leis gerais que abordam o tema incidentalmente, a

exemplo, da Lei n. 9.507/97, denominada Lei do *Habeas data*. Esta lei se refere apenas ao direito de solicitar, retificar e complementar informações a respeito do titular. Em 2014, entrou em vigor a Lei n. 12.965, denominada popularmente de Marco Civil da Internet. No entanto, muito embora esta lei dedique uma parte à proteção de dados pessoais, não tratou da matéria de forma específica, mas apenas de modo geral e superficial, como as demais legislações existentes até então.

Dessa forma, a presente pesquisa se mostra relevante do ponto de vista jurídico, considerando que o Brasil até 2018 era o único país do Mercosul a não ter uma legislação de proteção de dados pessoais. Assim, investigar-se-á neste trabalho se, de fato havia necessidade na aprovação de lei de proteção de dados pessoais, como forma de possibilitar o controle das informações pessoais por parte de seus titulares.

Para alcançar os objetivos propostos, opta-se pela realização de um trabalho que será desenvolvido na abordagem qualitativa e quantitativa. Os dados coletados nesta pesquisa serão predominantemente descritivos, uma vez que o material obtido é rico em descrições de fatos, acontecimentos e decisões jurisprudenciais.

O tipo de busca será o bibliográfico, fazendo-se um levantamento da bibliografia publicada, tanto nacional como alienígena, incluindo revistas cientificas, periódicos, que possam fornecer conhecimentos acerca do objeto da investigação. Utilizar-se-á ainda, a técnica de pesquisa documental, valendo-se de materiais que não receberam tratamento analítico, como artigos científicos, reportagens de revistas e documentos internacionais de proteção de dados pessoais.

Para a realização desta pesquisa serão utilizados ainda, os seguintes métodos: dedutivo, histórico e comparativo. No método dedutivo, parte-se das teorias que explicam os direitos da personalidade para se chegar à conclusão da privacidade como direito personalíssimo. O método histórico se revela importante

neste trabalho, pois analisar-se-á tanto a evolução histórica dos direitos da personalidade como o direito à privacidade.

Quanto ao método comparativo, será realizado estudo entre os modelos europeu e norte-americano, assim como aqueles dos países do Mercosul que já possuem lei de proteção de dados pessoais, para se averiguar que modelo se revela como adequado e satisfatório.

O trabalho ordenar-se-á em quatro capítulos: No primeiro, apresentar-se-á o assunto, aludindo-se à evolução histórica dos direitos da personalidade e a cláusula geral de tutela da pessoa. Nesse capítulo, será analisada a personalidade como valor e as situações jurídicas existenciais, para posteriormente demonstrar a correlação entre a privacidade com a estrutura da propriedade, assim como o conceito contemporâneo de privacidade.

No segundo capítulo, far-se-á a análise da correlação da tutela da privacidade e a informação, tendo em vista que atualmente a informação é considerada um bem jurídico de valor extraordinário, noção indispensável para compreensão do presente tema. Antes de tal demonstração, faz-se necessário constatar a íntima cumplicidade entre a privacidade e a intimidade, que apesar da divergência existente na doutrina, acerca de se considerarem conceitos distintos ou idênticos, ambos pretendem tutelar a pessoa humana. Em seguida, buscar-se-á saber se o direito à privacidade deve ser considerado como direito geral ou deve ser entendido nas suas diversas facetas. Ao final deste capítulo, pretende-se identificar as situações em que a cessão da informação é indispensável, muito embora necessite de igual proteção.

Na sequência, estudar-se-á no terceiro capítulo a questão da proteção de dados pessoais, voltando-se ao direito comparado para expor como se aborda tal temática no contexto jurídico internacional. Será dado enfoque ao modelo europeu, que tem sido considerado paradigmático no que se refere à tutela de dados pessoais. No entanto, analisar-se-á também o modelo italiano, que por ter sido um dos últimos países da Europa a legislar sobre a

matéria, conseguiu absorver melhor as experiências de outros países acerca desta matéria.

O modelo norte-americano também será objeto de estudo neste capítulo, por se considerar a origem do direito à privacidade. Demonstrar-se-á a preferência das legislações, sobretudo a europeia por princípios, identificando-se o significado de cada um no contexto da proteção de dados pessoais. Serão também objeto de reflexão alguns conceitos utilizados nestas legislações, tais como: dados pessoais, dados sensíveis, tratamento, autodeterminação informativa, direito de oposição e todos os princípios aplicados à presente temática.

O último capítulo centrar-se-á na proteção de dados pessoais no Brasil, identificando as legislações que tratam do tema, mesmo que de forma genérica. Serão objeto de análise as leis do *Habeas Data* e o Marco Civil da Internet. No entanto, o foco principal deste capítulo será o estudo crítico-reflexivo dos principais aspectos da Lei geral de proteção de dados pessoais no Brasil, recém aprovada e sancionada.

Por fim, esse estudo segue os referenciais da doutrina civil-constitucional, considerando que a privacidade é aqui analisada como direito fundamental e da personalidade, assim como ao recente ramo do direito chamado sociedade da informação. Pretende-se assim, contribuir para o fortalecimento dos direitos da personalidade, em especial para o enriquecimento da discussão sobre o direito à privacidade no tratamento de informações pessoais constantes em bancos de dados privados.

1

A tutela da personalidade e a expansão do conceito de privacidade

Revela-se controversa na doutrina a origem da tutela da pessoa, no entanto, mostra-se como consenso o fato de que somente com o pensamento doutrinário, sobretudo o alemão do século XIX, iniciou a construção da teoria dos direitos da personalidade, todavia, alguns antecedentes históricos merecem ser lembrados para que se possa sistematizar a temática na sua trajetória evolutiva (TEPEDINO, 2004, p. 24).

Como antecedente importante, pode-se identificar o pensamento greco-romano, considerado o ponto de partida para o estudo dos direitos da personalidade, bem como encontram-se lá as maiores contribuições para a construção destes direitos, no entanto, sabe-se que na Antiguidade Clássica, a pessoa não era protegida de forma integrada, não tinha uma tutela com a mesma intensidade que nos moldes atuais.

No direito romano, por exemplo, os homens ou eram livres ou eram escravos. A personalidade jurídica só era dada aos livres, que dispunham do chamado *status libertatis*. Os escravos eram considerados *res,* mercadoria, e não poderiam praticar os atos jurídicos em seus próprios nomes, mas sim em nome de seus donos (CAPELO DE SOUSA, 2011, p. 47).

O fato é que a proteção da pessoa humana, especialmente no campo privatístico foi assimilada com dificuldades, isto ocorria porque os Códigos Civis que seguiram o *Code Napoléon,* e a

doutrina trataram de forma muito tímida esta matéria, não obstante o reconhecimento de que alguns aspectos da proteção da personalidade tenham se desenvolvido entre os séculos XIX e XX. Como marco fundamental para a proteção deste direito deve ser reconhecida a Constituição de Weimar, de 1919, que será analisada neste capítulo.

Nos dias atuais, praticamente todos os ordenamentos dos Estados Democráticos de Direito reconhecem a pessoa humana como centro e fim da ordem jurídica, representando grande evolução na história da tutela da pessoa humana, manchada pela ignomínia da escravidão, bem como pelas barbáries nazi-fascistas.

A noção de privacidade com todos os sentidos que se apresenta não é também tão recente, podendo ser identificada em outras épocas e em outras sociedades. Entretanto, somente no final do século XIX passou a assumir suas atuais feições no ordenamento jurídico.

Neste capítulo analisar-se-á a evolução histórica dos direitos da personalidade, como também a privacidade como direito fundamental da personalidade, demonstrando que o despertar da privacidade ocorreu num período em que a percepção da pessoa humana pelo ordenamento foi modificada, passando a ocupar papel central na ordem jurídica.

1.1 A evolução histórica do direito da personalidade e a cláusula geral de tutela da pessoa.

A construção da teoria dos direitos da personalidade é recente, porém a ideia de proteção da pessoa humana não parece ser tão recente assim. Podem-se encontrar várias formas de proteção, desde o direito grego, com as *dike kakegorias,* passando pelo direito romano, com a *vidicatio libertatis,* pela qual se obtinha uma declaração que atestava se uma pessoa era livre ou não; o instituto da *potestas in se ipsum,* em que alguns romanistas tentaram demonstrar que o direito romano concederia ao homem

uma espécie de direito de propriedade sobre seu próprio corpo (DONEDA, 2006, p. 66-67).

É possível citar como antecedente dos direitos da personalidade, a a*ctio iniuriarum aestimatoria,* como sendo uma ação destinada a repelir algumas espécies de atentados físicos ou morais contra o cidadão romano. Esta ação é característica da época clássica romana que se iniciou no séc. II a.C até 284 d.C., abrangendo o período pré-imperial até o Alto Império.

Por intermédio da *actio iniuriarum,* o pretor tinha total liberdade para julgar a extensão da injúria, graduando assim, uma sanção em pecúnia. Nesse sentido, através do direito pretoriano se ultrapassaram as influências da Lei das XII Tábuas em matéria de direito da personalidade, tendo em vista que o refinamento cultural do povo romano gerou descontentamento em relação às penas taliônicas (CAPELO DE SOUSA, 2011, p.48-49).

Capelo de Souza (2011, p. 48) esclarece que "o direito Greco-romano é considerado ponto de partida para o estudo dos direitos da personalidade, isto aconteceu porque lá se encontram as maiores contribuições para a teoria dos direitos da personalidade". A expressão *dike,* em grego, representa uma concepção de justiça, baseada na ideia de igualdade, contrapondo-se à *themis,* que também representava a justiça, a partir de uma noção aristocrática da representação de uma vontade superior.

A tutela da personalidade na Grécia antiga se fazia através da *Hybris, q*ue significava a ideia de injustiça, excesso, desequilíbrio em face da pessoa. Era uma ação punitiva de natureza penal que vedava qualquer excesso cometido por um cidadão contra outro, proibia maus tratos contra a pessoa humana, bem como repudiava contra qualquer forma de injustiça (SZANIAWSKI, 2005, p. 24).

Com o pensamento filosófico greco, segundo Capelo de Souza (2011, p. 47), o homem passou a ser tido como origem e finalidade da lei e do direito. Dessa forma, o homem é o destinatário primeiro e final da ordem jurídica, conferindo um novo sentido à personalidade e a seus direitos.

Percebe-se que o homem, na Grécia Antiga era o centro referencial do ordenamento, como inclusive hoje é concebido. Hodiernamente, a dignidade da pessoa humana foi eleita como valor máximo e fundamento do Estado Democrático de Direito.

Na Grécia havia uma certa interpenetração do público e do privado, pois os cidadãos reunidos na ágora participavam de grandes decisões envolvendo os interesses da comunidade, quer votando leis, quer julgando seus semelhantes em processos públicos de maior importância. Percebe-se que já em Roma vai ocorrer uma separação mais nítida entre as esferas pública e privada, havendo pouca participação dos cidadãos na esfera pública (FACCHINI NETO, 2003, p.16-18).

Ao longo de toda a história do direito romano, os estatutos jurídicos das pessoas foram extremamente diversificados, segundo Capelo de Sousa:

> Só tinha capacidade jurídica, e consequentemente integrais direitos de personalidade, quem possuísse os três *status: o status familae* (com a inerente qualidade de *pater-familias),* o s*tatus civitatis (*ou seja, a categoria de cidadão, que era desde logo negada aos estrangeiros e aos escravos e cuja plenitude muito custou a alcançar aos plebeus) e o *status libertatis* (ou seja, a qualidade de pessoa livre, que era condição, embora não suficiente, da cidadania) (CAPELO DE SOUSA, 2011, p.47).

É importante esclarecer que apesar de o pensamento Greco-romano ser considerado o embrião da teoria geral da personalidade, grande parte da doutrina entende que no direito romano não se cuidava da proteção aos direitos da personalidade, como atualmente se tutela, levando-se em consideração que o seu contexto histórico-social é totalmente diverso (SZANIAWSKI, 2005, p. 31).

Nesse sentido, Doneda (2006, p.67) adverte que na Antiguidade Clássica, a pessoa não era protegida em perspectiva

integrada, não havendo sequer uma categoria que pudesse ser relacionada com a atual noção de personalidade.

O referido autor esclarece ainda que:

> os discursos neste sentido apresentam um erro de perspectiva, ressaltando, desmesuradamente a amplitude do caráter humanista da antiguidade clássica ao entendê-lo à estrutura jurídico-política – o que não raro ocorre em certas perspectivas que talvez padeçam de excessivo romantismo (DONEDA, 2006, p. 67).

Assim, pode-se concluir que na Antiguidade não se tinha uma tutela da pessoa com a mesma intensidade e nos mesmos moldes que se tem atualmente, considerando que havia muitas diferenças sociais, as quais determinavam que tratamento seria dispensado à pessoa (TEPEDINO, 2004, p. 24).

Nesse sentido, Sarlet (2006, p. 30) sustenta que "no pensamento filosófico e político da antiguidade clássica, verifica-se que a dignidade (d*ignitas)* da pessoa humana dizia, em regra, com a posição social ocupada pelo indivíduo e o seu grau de reconhecimento pelos demais membros da comunidade".

Foi a partir do humanismo, do século XVI, que se começou a afirmar a independência da pessoa e a intangibilidade dos direitos humanos. Assim, é importante lembrar a contribuição do humanista Mirandola (1986, p. 52-53) que influenciado pelo pensamento tomista, afirmou ser a personalidade humana um valor próprio, inato, expresso justamente na sua ideia de dignidade do ser humano, que nasce na qualidade de valor natural, inalienável e incondicionado.

A construção da noção de dignidade da pessoa humana teve como base o cristianismo, ao reconhecer no ser humano um princípio divino e eterno. Entretanto, foi com Kant (1980, p. 134-141) "que a ideia de dignidade da pessoa se desenvolveu e se

laicizou, como um atributo intrínseco ao homem sujeito dotado de autonomia, a quem se credita valor e não preço".[1]

Contrapondo-se à ideia de Kant acerca da noção de dignidade da pessoa humana, pode-se citar Hegel (1991), na sua Filosofia do Direito, para quem a dignidade constitui uma qualidade a ser conquistada. Hegel acabou por sustentar uma noção de dignidade centrada na ideia de eticidade, de tal sorte que o ser humano não nasce digno, tornando-se digno a partir do momento em que assume sua condição de cidadão. (SARLET, 2006, p. 36).

Percebe-se que Hegel com a sua concepção de dignidade se afasta de Kant e da expressiva maioria de autores ao não fundar a sua concepção de pessoa e dignidade em qualidades inerentes a todos os seres humanos (SARLET, 2006, p. 37).

Dessa forma, o pensamento medieval lançou as sementes de um conceito moderno de pessoa humana baseado na dignidade e na valorização do indivíduo como pessoa, entretanto, ainda não se conferiu relevo aos direitos dela.

Entende-se que após as duas grandes guerras, as atrocidades cometidas contra os indivíduos, serviram para apresentar ao mundo a necessidade inquietante e imediata da proteção da pessoa humana, passando o Estado e a própria sociedade a se preocuparem em reconhecer a importância da necessidade de tutela dos direitos da personalidade.

Essas novas ideias conduziram os juristas da época à formulação do direito geral de personalidade, como um *ius in se ipsum* - teoria do direito sobre si mesmo (SZANIAWSKI, 2005, p. 38).

O Renascimento e o Humanismo, segundo Capelo de Souza (2011, p. 61-62), contribuíram para construir a rampa de lançamento de um direito geral de personalidade, entendido como um *ius in se ipsum,* que não deixaria de estar presente na reflexão

[1] Acerca do conceito de Dignidade da Pessoa Humana em Kant ver SANTOS, Fernando Ferreira dos. **O Princípio Constitucional da Dignidade da Pessoa Humana**. Fortaleza: Celso Bastos, 1999.

jurídica da tutela da personalidade humana. Com o *ius in se ipsum,* o homem teria direito de fazer de si o que melhor lhe conviesse, ressalvadas as proibições expressas em lei, como a automutilação e sujeição voluntária à tortura.

Os chamados direitos naturais ou inatos também contribuíram para o surgimento dos direitos da personalidade a partir do século XVII, afirmando a existência de direitos que nascem com o homem, indissoluvelmente ligados à pessoa, são preexistentes ao seu reconhecimento pelo Estado. Nesse sentido, Vasconcelos (2010, p.57) explica que os direitos humanos ou naturais são atributos que o homem fatalmente carrega condigo, como o espírito que habita seu corpo, como sangue que lhe circula nas veias, independendo de tempo, lugar, raça ou qualquer outra circunstância.

A ideia de direitos naturais inalienáveis aparece no pensamento do século XVII, com as obras de Hugo Grócio, Samuel Pufendorf, Thomas Hobbes e John Milton. Milton ainda reivindicou o reconhecimento dos direitos de autodeterminação do homem, de liberdade de manifestação e supressão da censura (SARLET, 2005, p. 46).

John Locke, pensador do século XVIII, sofreu influência dos seus antecessores, reconhecendo os direitos naturais inalienáveis do homem, entretanto, defendeu a sua oponibilidade em frente aos detentores do poder, em face do contrato social e identificou o direito de resistência como um dos direitos naturais do homem (SARLET, 2005, p. 46-47).

A concepção de direitos inatos tem uma origem histórica, que se radica nas condições em que se criaram quando da compreensão e absorção do indivíduo pelos poderes absolutos, surgindo assim, a pressuposição de um estado primitivo de existência, ao qual deveriam ter correspondido os direitos inatos.

Nesse contexto, a teoria dos direitos inatos foi à consequência da reação contra o superpoder do Estado de Polícia,

estando na base das Declarações dos Direitos do Homem e do Cidadão, em 1789.

Para a contextualização da presente temática, são de grande importância os antecedentes históricos aqui analisados, todavia, a efetiva construção dos direitos da personalidade se deu com a doutrina europeia, sobretudo a alemã, da segunda metade do século XIX.

Doneda (2006, p. 73) esclarece que a proteção da pessoa no ordenamento, mais ainda no campo privatístico, foi assimilada com dificuldade. Os códigos civis que seguiram o *Code Napoléon* por mais de um século foram muito tímidos neste aspecto, sem contar a timidez de grande parte da doutrina em apregoar um sistema no qual os direitos da personalidade encontrassem efetiva cidadania. A doutrina tinha opinião de que a proteção da pessoa fosse função do direito público, de acordo com o pensamento jurídico e social da época.

Com a ascensão da burguesia houve a separação dos interesses econômico-privados dos interesses político-públicos, com uma acirrada dicotomia entre as duas esferas. Era necessário traçar a distinção entre público e privado para que nada de particular prejudicasse a vontade geral da nova nação.

O Direito Privado passou a ser disciplinado amplamente pelo legislador, surgindo assim, uma legislação influenciada pela ideologia burguesa. Em 1804, surgiu o Código Civil Francês, seguindo-se cem anos depois, o Código Civil alemão. Eis aí a era da codificação.

Dessa forma, Moraes (1993, p. 1) afirma que o Direito Civil clássico identificava-se com o direito inserto no Código de Napoleão, tendo seu conteúdo delimitado através da sistematização que separou as leis civis das públicas.

O marco característico do processo de proteção da personalidade deve ser reconhecido na Constituição da República Federal da Alemanha de 1919, pois repercute até hoje no constitucionalismo moderno, merecendo especial atenção no que

diz respeito às relações entre a Constituição e o direito privado. Foi a Constituição de Weimar que englobou em âmbito constitucional os institutos de direito privado, como família, propriedade, empresa e contrato (DONEDA, 2006, p. 74).

A partir da segunda guerra mundial, o debate constitucional passou a incluir a tomada de posição do ordenamento em relação aos centros de interesses pessoais e patrimoniais e a Constituição de Weimar reconheceu que a tutela dos interesses econômicos somente seria legítima enquanto estivesse vinculada aos direitos da pessoa.

Assim, foi inaugurado um novo momento do constitucionalismo, com a posição de predominância da Constituição no vértice normativo. Dessa forma, os interesses constitucionalmente protegidos não poderiam ser violados por normas inferiores à Constituição.

O Código Civil não poderia mais se apresentar como um sistema exaustivo em matéria de Direito Civil, ganhando vigor a discussão em torno da *summa diviso* entre direito público e direito privado. A realidade com a qual o ordenamento estava acostumado a conviver não encontrava mais as suas referências em um terreno construído em torno do paradigma da *summa diviso* (DONEDA, 2005, p. 74).

O Direito Civil passou a se preocupar com a tutela da pessoa em um sentido amplo, revelando-se assim, significativa mudança na sua concepção originária, isto porque sofreu forte influência das codificações oitocentistas, que tinham como base o contrato e a propriedade, tutelando apenas os aspectos patrimoniais da vida em sociedade.

Essa mudança de paradigma foi interpretada por alguns autores, como Giorgianni (1998, p. 35), como sendo certa a morte deste modelo na primeira metade do século XX. O Código Civil não mais representava a continuidade de uma tradição que separava os interesses individuais das questões de interesse da comunidade.

O Direito Civil passou a considerar o homem e a sociedade em seu todo, o que culminou com o aumento do número de problemas a ser solucionados, tendo institutos tradicionais perdido a sua estabilidade, por terem sido obrigados a responder a demandas mais complexas, tais como: a propriedade que deixou de ter caráter absoluto, a autonomia da vontade, tendo sofrido limitações pela função social do contrato e outros exemplos que não cabe aqui ser discutidos.

A inclusão dos direitos da personalidade ao direito civil representa essa mudança no paradigma privatístico, que se preocupava com questões de natureza patrimonial, passando a preponderar às questões existenciais. Assim, a personalidade em seus vários aspectos, como o nome, a honra, a imagem e outros, acabaram sendo compreendidos pelo Direito Civil como direitos subjetivos da pessoa, que em caso de ofensa, ensejaria uma reparação.

Nesse sentido, alguns juristas começaram a inventariar os direitos da personalidade previstos pelo ordenamento, tornando uma solução frequente classificá-los, particularizá-los, diferenciando-os dos demais direitos subjetivos. Entretanto, o direito subjetivo, em sua estrutura clássica pressupõe a existência de um objeto, externo ao sujeito, o que não ocorre com os direitos da personalidade, que recaem sobre aspectos indissociáveis de seu titular.

Com isso, diversos problemas foram surgindo, e um deles referente à qualificação de sujeito de direito como o próprio objeto dos direitos da personalidade, mostrando-se desconfortável para uma grande parte da doutrina, tendo como um dos defensores desta concepção, Perlingieri (2007, p. 155), que entende nesta matéria não se poder aplicar o direito subjetivo, elaborado na categoria do "ter", pois na categoria do "ser" não há dualidade entre sujeito e objeto, porque ambos representam o ser.

Já Cupis (2008, p. 33) afirma que o objeto dos direitos da personalidade não é exterior ao sujeito, ao contrário dos outros

bens que são possíveis objetos de direito. Esta não exterioridade não significa identidade, visto que o modo de ser da pessoa não é a mesma coisa que a pessoa.

Cupis (2008, p. 30) é um dos defensores da tese de pluralidade de direitos da personalidade, tendo admitido em sua obra *Os Direitos da Personalidade,* que a individualização do bem resulta na individualização das necessidades, sendo a exigência distinta da liberdade, e a necessidade de se viver respeitado, não se confunde com a necessidade de se distinguir das outras pessoas. Concluindo, que são também distintos os bens correspondentes. A consciência comum para Cupis (2008, p. 33) "não costuma distinguir um só bem na pessoa; pelo contrário, reconhece vários bens distintos, na vida, na honra, na identidade, e outros, da pessoa".

Nesse contexto, surge uma discussão na doutrina dos direitos da personalidade: os direitos da personalidade devem ser concebidos como uma pluralidade de direitos, onde cada um incidiria sob um aspecto da personalidade, ou existe um único direito de personalidade, referindo-se à personalidade como um todo, um direito geral de personalidade? Esse questionamento gerou controvérsias na doutrina clássica, no entanto, atualmente parece não haver discordâncias na doutrina contemporânea.

A teoria que sustenta uma pluralidade de direitos da personalidade aponta duas concepções ditas atomísticas: a primeira, aquela que considera uma série aberta de direitos, ou seja, uma atipicidade de direitos da personalidade; e a segunda, uma série fechada de direitos, isto é, tipificados ou *numerus clausulus*.

Contrapondo-se às concepções ditas atomísticas dos direitos de personalidade, surge a teoria monista, cujos adeptos defendem os direitos da personalidade na forma de um direito único, originário e geral, concretizando a tutela geral da personalidade, apoiando-se na ideia de concepção do valor unitário da pessoa humana e da sua dignidade.

Nesse sentido, Perlingieri ensina que:

> {...} O fato de a personalidade ser considerada como valor unitário, tendencialmente sem limitações, não impede que o ordenamento preveja, autonomamente, algumas expressões mais qualificantes como, por exemplo, o direito à saúde (art. 32 Const.), ao estudo (art. 34 Const.), ao trabalho (at. 35 ss. Const.). O juiz não pode negar tutela a quem peça garantias sobre um aspecto da sua existência que não tem previsão específica, porque aquele interesse já tem uma relevância ao nível de ordenamento e, portanto, uma tutela também em via judicial (art. 24 Const.) (PERLINGIERI, 2007, p.156).

As teorias tipificadoras dos direitos da personalidade não encontram mais muitos adeptos, tendo em vista a evolução da teoria dos direitos da personalidade, visto que a admissão de uma tutela geral tem sido uma tendência mundial.

Entretanto, a teoria que admite uma série atípica de direitos de personalidade ainda encontra muitos adeptos, como por exemplo, a doutrina francesa, que reconhece uma série ampla de direitos isolados da personalidade, a partir da aplicação da norma que gera o dever de indenizar em hipótese de lesão a algum bem da personalidade, sustentando o caráter não taxativo das listas de direitos da personalidade.

A doutrina espanhola também é adepta da teoria atomística que admite uma série de direitos dos quais decorrem outros atípicos, dividindo-os em duas categorias: os direitos relativos à existência física ou inviolabilidade corporal; e os relativos à moral (TOBEÑAS, 1952, p. 34-60).

No direito português, alguns autores, como José de Oliveira Ascensão (1997, p. 78), sustentam que a admissão de um direito geral de personalidade oferece algumas desvantagens, como por exemplo, causar insegurança jurídica, por ser um direito de desmesurada extensão. Entretanto, as teorias atomísticas estão em franca decadência, posto que não conseguiram justificar as críticas que lhe foram lançadas.

No Brasil, podem-se encontrar diversas classificações dos direitos de personalidade. Gomes (2001, p. 153-154) classificou-os em dois grupos: os direitos à integridade física e os direitos à integridade moral, afirmando que os direitos de personalidade sempre cabem em uma dessas categorias. Já Pontes de Miranda (2000, p. 37) divide os direitos de personalidade em: direito à vida, à integridade física, à integridade psíquica, à liberdade, à honra à imagem, à igualdade, ao nome, à intimidade e ao direito autoral.

Bittar (2006, p. 17) classifica tais direitos em físicos, ou de integridade corporal, que compreendem o corpo, como um todo, os órgãos, os membros; os direitos psíquicos, que são aqueles relativos aos elementos intrínsecos da personalidade e direitos morais, compreendendo a liberdade, a intimidade e o sigilo.

Todas essas teorias tipificadoras dos direitos da personalidade sofrem críticas, pelo fato de que nem mesmo seus adeptos conseguiram aclarar o tema, a partir de suas classificações, isto porque não há como criar uma classificação absolutamente cientifica que abarque todos os direitos possíveis.

Na opinião de Szaniawski (2005, p.123-124), o fracasso das teorias tipificadoras foi o fato de estarem atreladas à distinção entre direitos públicos e direitos privados da personalidade, e na verdade seriam os mesmos, mas em ambientes protetivos diversos, bem como a exigência de que tais direitos estejam positivados no Código Civil, o que se justifica pelo apego aos sistemas fechados do século XIX.

O fato é que, com os fenômenos da publicização, constitucionalização e repersonalização do Direito Privado, bem como pela eleição da dignidade da pessoa humana como valor fundamental dos Estados Democráticos de Direito, recolocando o ser humano no centro do sistema, não há mais que se falar em dicotomia entre o público e privado.

Dessa forma, estes fenômenos trazem a lume um direito geral de personalidade. Somente por meio de uma cláusula geral de tutela ou de um direito-mãe pode-se permitir uma construção

jurisprudencial capaz de enfrentar as diversas modalidades de lesão à personalidade.

Nesse contexto, Perlingieri (2007) ensina que ao lado da técnica de legislar com normas regulamentares, através de previsões específicas, coloca-se a técnica de cláusulas gerais. Legislar por cláusulas gerais significa deixar ao juiz, ao intérprete, uma maior possibilidade de adaptar a norma às situações de fato.

Resta demonstrado que somente a tutela da pessoa pelos direitos da personalidade tem como abarcar a complexidade das situações que envolvem a personalidade humana, sendo a única a tutelar de forma adequada a pessoa humana, permitindo uma tutela em uma perspectiva globalizante, não excludente, abrangendo mesmo os bens não previstos em lei.

Analisando as teorias tipificadoras ou pluralistas, bem como aquelas que reconhecem um direito geral de personalidade, Menezes e Gonçalves (2012, p. 177-178) destacam que o Código Civil Brasileiro, apesar de não ter feito menção expressa ao direito geral da personalidade, optando por especificar alguns direitos especiais, admite uma ampla possibilidade ressarcitória, prevista no art. 927, *caput,* e parágrafo único do mesmo Código. Por esta razão as referidas autoras acreditam na presença de uma verdadeira cláusula geral de tutela da pessoa.

Tal fato se justifica, considerando-se que se os direitos especiais de personalidade, previstos no Código Civil brasileiro já são assemelhados aos direitos fundamentais, muito mais seria a cláusula geral de tutela da pessoa, isto porque tem fina proximidade com os direitos humanos (MENEZES; GONÇALVES, 2012, p. 178).

A cláusula geral de tutela da pessoa, expressão utilizada por Perlingieri (2007, p. 156) entende a personalidade não como um direito, mas como um valor fundamental do ordenamento jurídico. Para o referido autor, o fato de a personalidade ser considerada como valor unitário, não impede que o ordenamento preveja algumas expressões mais qualificadas, como, por exemplo, direito à

saúde, ao estudo, ao trabalho. Já o direito geral de personalidade é uma norma aberta do direito privado, que tem como finalidade salvaguardar a pessoa humana em qualquer circunstância.

Na próxima seção, considerando-se a pertinência e a importância do estudo da personalidade como valor, bem como situação jurídica existencial, analisar-se-ão as principais diferenças entre personalidade e capacidade, assim como a possibilidade de aplicação da categoria dos direitos subjetivos aos direitos da personalidade, afastando-se toda e qualquer interpretação que identifique estes direitos com interesses meramente patrimoniais.

1.2 A personalidade como valor e as situações jurídicas existenciais

Para o Direito Civil tradicional, a personalidade é entendida como a possibilidade de ser sujeito de direito, titular de direitos e obrigações. Dessa forma, a personalidade acabou sendo confundida com a ideia de capacidade de direito. Fato esse que se observa até hoje na maior parte da doutrina civilista. Autores como Pontes de Miranda (2000), Rodrigues (2002) e Diniz (2004) comungaram desta mesma ideia, no sentido de que a personalidade e a capacidade jurídica são expressões sinônimas.

Já Capelo de Souza (2011, p. 106-107) entende que personalidade e capacidade são conceitos interpenetrados e conexos, mas que não podem ser confundidos, na medida em que os valores jurídicos que estes institutos incorporam são reabsorvidos também no bem jurídico da personalidade, como objeto da tutela geral referida.

Na verdade, boa parte da doutrina faz distinção entre personalidade e capacidade. Entretanto, há uma dificuldade de mudança de perspectiva diante de uma confusão conceitual que se manteve dominante no pensamento jurídico por muito tempo e só se desfez recentemente.

É necessidade premente reconhecer a personalidade como um valor que se expressa para além da mera capacidade de adquirir direitos e contrair obrigação. Por esta perspectiva, pretende-se uma ruptura com as concepções patrimonialistas, que no século XIX negaram a existência dos direitos da personalidade.

Dantas (2001, p. 152) ensina que, quando se fala em direitos da personalidade não se está a identificar a personalidade, com a capacidade de ter direitos e obrigações, e sim a personalidade como um fato natural, como um conjunto de atributos inerentes à condição humana.

O fato é que atualmente não mais se discute a existência ou não dos direitos da personalidade, a afirmação destes direitos foi de extrema relevância em frente aos progressos científicos e tecnológicos observados na atualidade.

Nesse sentido, diante deste progresso tecnológico é que surge a discussão acerca do tratamento de informações pessoais por agentes privados (bancos de dados), sem o conhecimento e autorização do seu titular. A tutela da personalidade nesses casos se mostra absolutamente suscetível de violação, considerando a fragilidade do sistema de controle dessas informações. Este aspecto da personalidade será aprofundado mais à frente, não cabendo nesse momento maiores discussões.

Conforme foi mencionado anteriormente, outra questão problemática na seara dos direitos da personalidade dizia respeito à sua conformação como direitos subjetivos. Criticava-se a possibilidade de o homem ser considerado sujeito e objeto da mesma relação jurídica

Assim, os que negavam a possibilidade de aplicação da categoria dos direitos subjetivos aos direitos da personalidade também argumentavam que o direito subjetivo havia sido elaborado, tradicionalmente, para a tutela de interesses pertinentes à esfera do *ter,* e não do s*er,* ou seja, para a proteção do patrimônio (MEIRELLES, 1998, p. 18).

Nos direitos da personalidade, os objetos de tutela são indissociáveis de seu titular e por isso não se admitia tutelar interesses existenciais de uma posição jurídica tradicionalmente voltada para a disciplina de interesses patrimoniais.

Nesse contexto, Perlingieri esclarece que:

> Contrapõem-se, tradicionalmente, duas definições de direito subjetivo: direito subjetivo como poder de vontade e direito subjetivo como interesse protegido. A disputa entre os defensores das duas teorias subtende diversas avaliações e diversas ideologias; nela se espelha as diversidades entre as concepções liberalistas e as primeiras tentativas de entender o direito de um ponto de vista teleológico. A definição corrente salda os dois aspectos: o direito subjetivo é, afirma-se usualmente, o poder reconhecido pelo ordenamento a um sujeito para realização de um interesse próprio do sujeito (PERLINGIERI, 2007, p. 120).

Merece destaque que, além de uma reavaliação na noção de direito subjetivo, também reclamou-se o alargamento do conceito de bem, isto porque o direito subjetivo se divide em três elementos: sujeito, objeto e relação jurídica (PEREIRA, 2006, p.42). Assim, o objeto, tradicionalmente, foi reduzido aos bens patrimoniais. Todavia, admitindo-se a tutela de interesses existenciais, o objeto da relação pode ser um bem extrapatrimonial.

Não obstante se entenda que a aplicação dos direitos da personalidade por meio dos direitos subjetivos não se revela adequada, visto que no momento atual, tem-se a dignidade da pessoa humana como centro de todas as discussões que envolvem o direito, é importante mencionar que há quem entenda, como Cupis (2008, p. 24-25), que não há uma impossibilidade lógica em se aceitar que os direitos da personalidade constituem direitos subjetivos, nem tão pouco, que os direitos da personalidade tenham como objeto os atributos físicos ou morais da pessoa, isto acontece porque o sistema jurídico não pode se limitar a tutelar apenas a esfera do *ter,* deixando de fora o *ser,* já que esta tutela os bens mais preciosos da personalidade humana.

Em outro sentido, Moraes (2010, p. 112) entende que não há que se falar exclusivamente em direitos subjetivos da personalidade, mesmo se atípicos, porque a personalidade humana não se realiza apenas através de direitos subjetivos, mas sim mediante uma complexidade de situações jurídicas subjetivas que podem apresentar-se, sob as mais diversas configurações.

Moraes arremata:

> {...} o atual ordenamento jurídico, em vigor desde a promulgação da Constituição Federal de 5 de outubro de 1988, garante tutela especial privilegiada a toda e qualquer pessoa humana, em suas relações extrapatrimoniais, ao estabelecer como princípio fundamental, ao lado da soberania e da cidadania, a dignidade humana. Como regra geral daí decorrente, pode-se dizer que, em todas as relações privadas nas quais venha a ocorrer um conflito entre uma situação jurídica subjetiva existencial e uma situação jurídica patrimonial, a primeira deverá prevalecer, obedecidos, dessa forma, os princípios constitucionais que estabelecem a dignidade da pessoa humana como valor cardeal do sistema (MORAES, 2010, p. 114).

Dessa forma, não existe um número fechado de hipóteses tuteladas, como ensina Perlingieri (2007, p. 156), isto porque tutelado é o valor da pessoa sem limites. Assim, conclui que "a elasticidade torna-se instrumento para realizar formas de proteção também atípicas, fundadas no interesse à existência e no livre exercício da vida de relações".

Nesse contexto, a personalidade não é um direito, mas um valor fundamental do ordenamento, estando na base de uma série aberta de situações existenciais, nas quais se traduz a sua exigência de tutela, não assumindo necessariamente a forma de direito subjetivo, nem tão pouco existindo um número fechado de hipóteses tuteladas, pois tutelado é o valor da pessoa humana.

Moraes (2010, p. 112-120) adverte que a relevância dos direitos da personalidade decorre de fatores sociais, como a explosão de meios de comunicação de massa, progressivamente

direcionados a desconsiderar vidas particulares. Neste sentido, se inserem aí questões envolvendo o uso da internet, mais especificamente a manipulação de informações pessoais por bancos de dados, como uma afronta à privacidade das pessoas.

Dessa forma, nos Estados Unidos, onde a propriedade privada exerceu um papel central, a construção da *privacy* foi feita através de uma esfera de intimidade da pessoa, do mesmo modo que se faz com um pedaço de terra, ou seja, da violação-proteção de uma propriedade particular. Moraes (2010, p. 124), citando Alan Westin (1967), afirma que "o melhor meio de tutelar a privacidade é considerar a informação como propriedade da pessoa, de modo que possa, se desejar, negociá-la no mercado".

No Brasil, a privacidade ou a possibilidade de controle sobre os próprios dados pessoais, em especial os dados sensíveis, isto é, aqueles que dizem respeito à saúde, às opiniões políticas ou religiosas, a orientação sexual, têm como única proteção atualmente disponível o *habeas data,* instituto absolutamente insuficiente, posto que se destina à retificação de dados e não à disposição sobre os mesmos.

Ainda sobre a privacidade, Moraes (2010, p. 124), critica o Código Civil Brasileiro, no que se refere às relações extrapatrimoniais, entende que a legislação civil regrediu, isto porque se debate atualmente se, em virtude do princípio de proteção da dignidade humana, não deveria ter uma expansão da autonomia privada no que se refere às escolhas da vida privada de cada pessoa humana, ou seja, a privacidade garantida pela Constituição a uma pessoa digna deveria significar um mais amplo poder de escolha sobre os seus próprios bens.

Nessa perspectiva, reclamou-se que para a definição dos direitos da personalidade, além da releitura da noção clássica de direito subjetivo, era necessário o alargamento do conceito jurídico de bem. A noção de bem jurídico passou a ser compreendido como a totalidade dos bens corpóreos ou incorpóreos, vinculados à esfera

jurídica do sujeito, para se chegar à noção de bens da personalidade.

Amaral (2006, p. 249) explica que o objeto da relação jurídica pode ser uma coisa nas relações de direitos reais, pode ser uma ação humana nas relações obrigacionais e pode ser um atributo da própria pessoa nas relações que envolvem direitos da personalidade.

Já Capelo de Sousa, acerca da definição do bem da personalidade humana, adverte que

> O bem da personalidade humana juscivilisticamente tutelado como o real e o potencial físico e espiritual de cada homem em concreto, ou seja, o conjunto autônomo, unificado, dinâmico e evolutivo dos bens integrantes da sua materialidade física e do seu espírito reflexivo, sócio-ambientalmente integrado (CAPELO DE SOUSA, 2011, p. 117).

Percebe-se que o conceito de bem já não se confunde com o conceito de coisa, na medida em que a ampliação do conceito de bem se fez necessária, por não mais comportar a clássica definição como sendo suscetível de valoração pecuniária. Tal concepção estava em sintonia com as convicções de século XIX, considerando que o vínculo patrimonial representava expressão da própria personalidade humana.

Com a elevação da dignidade da pessoa humana como centro dos ordenamentos jurídicos, possibilitou-se a superação do paradigma patrimonialista vigente nos século XVIII e XIX. Assim, não havia mais a necessidade de os bens exprimirem um valor econômico, afirmando os direitos da personalidade como direitos subjetivos.

Szaniawski (2005, p. 70) esclarece que a personalidade que consiste na parte intrínseca do ser humano é o primeiro bem pertencente à pessoa, já que somente através dele se poderá adquirir os demais bens. A proteção conferida a estes bens

inerentes ao indivíduo se efetiva a partir dos direitos da personalidade.

Dessa forma, observa-se uma enorme divergência doutrinária acerca da ideia de direitos da personalidade como efetivos direitos subjetivos, assim como Amaral (2006) que considera os direitos da personalidade como direito subjetivo, que têm como particularidades inata e original, um objeto inerente ao titular, que é a sua própria pessoa, considerada nos seus aspectos essenciais. Por outro lado, aqueles que entendem, assim como Perlingieri (2007, p. 155) não ser adequada a aplicação dos direitos da personalidade como direitos subjetivos, por estes pertencerem a uma esfera patrimonial.

O que de fato importa para o presente estudo é a consideração da personalidade como um valor fundamental da ordem jurídica, constituindo-se na base de uma série de situações existenciais, que não necessariamente assumiram a forma de direito subjetivo, considerando que a pessoa humana não se realiza apenas através desta esfera.

Corroborando esta posição, Perlingieri (2007, p. 155) esclarece que "a pessoa se realiza não através de um único esquema de situações subjetivas, mas com uma complexidade de situações que ora se apresentam como poder jurídico (*potestá),* ora como interesse legítimo, ora como direito subjetivo, faculdade, poderes".

Assim, devem ser superadas as discussões dogmáticas sobre a categoria dos direitos da personalidade, pois a esta matéria não se pode aplicar o direito subjetivo elaborado sobre a categoria do "ter". Na categoria do "ser" não existe a dualidade entre o sujeito e o objeto, porque ambos representam o ser, e a titularidade é institucional, orgânica, como foi explicado anteriormente.

Não obstante a afirmação de que na esfera do "ser" não há dualidade entre sujeito e objeto, muitas vezes se confundem tais conceitos, como no caso "Pedrinho", menino sequestrado em hospital de Brasília-DF, em 1986, pela sua mãe adotiva, em que a

irmã se recusou a fazer o exame de DNA solicitado pela polícia[2]. Outro exemplo que bem retrata esta situação, representada pelo direito de personalidade sobre as partes do próprio corpo, é o caso de pessoa que disponibiliza material genético em clinica de reprodução assistida, para posterior utilização, considerando que passará por tratamento quimioterápico, no entanto a clínica perde tal material biológico.

1.3 A tutela da privacidade e sua correlação com a estrutura da propriedade

Percebe-se que de todos os direitos da personalidade, a privacidade foi o que mais sofreu transformações, desde o tradicional conceito elaborado por Warren e Brandeis como o "direito a ser deixado só", até a concepção atual, caracterizada pela liberdade de autodeterminação informativa, isto é, a capacidade de controlar as informações pessoais pelo seu titular (RODOTÀ, 2008, p. 24)

É importante destacar que neste trabalho utilizar-se-á o termo privacidade, embora, na doutrina brasileira existam vários termos para designá-la, como por exemplo, vida privada, intimidade, segredo, sigilo, dentre outros, fato este que parece ter sido influenciado pela doutrina alienígena, que também apontou para uma multiplicidade de alternativas.

A expressão "privacidade", segundo Doneda (2006, p. 107), tem raiz latina, mas por ser muito utilizado na língua inglesa, é chamado de anglicismo. Dessa forma, vê-se que o desenvolvimento do termo *"privacy*" na língua inglesa não encontrou paralelo em idiomas latinos.

[2] Entendendo como direito da personalidade das partes destacadas do próprio corpo, a autoridade policial pegou um filtro de cigarro utilizado pela moça, com a finalidade de fazer o DNA. A irmã alegou que se tratava de *res nullius (*coisa sem dono), ou seja, equiparou os direitos da personalidade à lógica patrimonialista, correlação esta que não se revela adequada nos dias atuais.

A Constituição Federal de 1988 utilizou as expressões "intimidade" e "vida privada", interpretando-se que a proteção da pessoa humana abrange ambos os aspectos. Neste contexto, Doneda esclarece que:

> {...} não é frutífero insistir em uma conceitualística que intensifique as conotações e diferenças semânticas dos dois termos. Cada um deles possui um campo semântico próprio: na "vida privada" encontraremos o discurso que proclama a distinção entre as coisas da vida pública e as da vida privada, no estabelecimento de limites, numa lógica que também é de exclusão. {...} O outro termo utilizado pelo constituinte, "intimidade", aparenta referir-se a eventos mais particulares e pessoais, a uma atmosfera de confiança (DONEDA, 2006, p. 109).

Na verdade, o problema trazido pela opção do legislador constituinte em utilizar os termos "vida privada" e "intimidade" é saber se são duas expressões distintas que devem ser valoradas de formas diferentes. Há autores como, Sampaio (1998, 269-274) que entende haver diversidade entre os termos e por isso propõe analisar as particularidades de cada um. Já Doneda (2006, p. 109-113) esclarece que a ausência de determinação terminológica na doutrina e jurisprudência pode ter sugerido ao legislador optar pelo excesso, até pelo temor de reduzir a aplicabilidade da norma.

O fato é que tanto a expressão "vida privada" quanto o termo "intimidade" pretendem o mesmo objetivo: tutelar a pessoa humana de forma mais ampla possível, considerando a complexidade das situações subjetivas existentes. Todavia, utilizar a expressão *privacidade* parece ser a opção preferida pela maior parte da doutrina, sendo a escolhida para ser utilizada nesta tese, conforme, foi mencionado anteriormente.

Doneda (2006, p. 111), citando a teoria dos círculos concêntricos de Hubman, adverte que os termos "vida privada" e "intimidade" fazem menção específica a determinadas amplitudes do desenvolvimento da proteção da privacidade, apresentando maior importância em determinado contexto histórico.

A doutrina de Hubman, constantemente citada, utiliza um esquema de esferas concêntricas com a finalidade de representar os diferentes graus de manifestação da privacidade, ou seja, ora como esfera da intimidade, ora como esfera privada e, em torno delas, a esfera pessoal. Vale destacar que a referida teoria foi desenvolvida e posteriormente abandonada pelo Tribunal Constitucional Alemão no que se refere à proteção de dados pessoais.

Insta observar que, quanto à quantidade de círculos ou esferas, não há consenso doutrinário, pois há quem entenda como Hubman, que só há duas esferas: a da intimidade e a da vida privada. No entanto, há também quem entenda que são pelo menos três as esferas ou círculos da privacidade. A esfera de maior diâmetro seria composta pela vida privada, consistente nos fatos e comportamentos que a pessoa não quer que se tornem públicos.

Na esfera da vida privada, pode-se encontrar um círculo um pouco mais reduzido, correspondente à esfera da intimidade, onde participam aquelas pessoas nas quais o indivíduo deposita certa confiança e com as quais mantém maior intimidade (COSTA JUNIOR, 2007, p. 30-32).

Segundo Costa Junior (2007, p. 36), na esfera mais interna da privacidade, pode-se encontrar o círculo do segredo, cujas informações são compartilhadas com poucas pessoas, aquelas muito chegadas. Assim, pode-se afirmar que a esfera da privacidade se divide em três círculos: a vida privada, a intimidade e a esfera do segredo.

Todavia, o referido autor adverte que o estabelecimento destas esferas não é rígido, isto porque as suas linhas divisórias são flexíveis e elásticas, dependendo da própria categoria social na qual o titular pertence ou até mesmo da sua profissão. Para se compreender a concepção atual de privacidade, faz-se necessário uma breve digressão histórica acerca de sua origem.

Durante a idade média, ainda não era possível reconhecer um sistemático anseio das pessoas pela privacidade ou isolamento. Alguns poucos privilegiados podiam-se isolar dos demais, como os

senhores feudais que o desejassem, ou então as pessoas que teriam optado pela solidão, como alguns religiosos, místicos.

Ao fim da idade média, Doneda (2006, p. 125) lembra que entre os senhores feudais bem colocados na sociedade havia manifestações que poderiam ser entendidas como indícios de surgimento de uma esfera privada em moldes similares aos atuais.

Somente no século XVI iniciou-se um processo de mudança de costumes, no que se refere à vida cotidiana, surgindo aí uma nova disposição arquitetônica das casas e cidades, tornando-se mais propícias à separação de classes e categorias, bem como mais favoráveis ao isolamento.

Parte da doutrina afirma que a origem do direito à privacidade remonta às teses filosóficas de Locke (2005) e Mill (2000). Locke desenvolveu sua ideia de liberdade como autonomia para dispor acerca de sua pessoa, de seus atos, de seus bens e de tudo quanto lhe pertença. Já Mill (2000) sustentava que os únicos aspectos da conduta humana que produziam deveres e responsabilidades sociais seriam aqueles que afetassem os demais. Para Mill, os aspectos que só dizem respeito ao indivíduo são absolutamente independentes, sendo o indivíduo soberano sobre si, seu corpo e sua mente.

É importante recordar que embora os autores acima citados tenham feito alusão a uma liberdade que pressupõe certo grau de autonomia, sem interferência de terceiros, naquela época não se utilizavam as expressões "privacidade", "intimidade" e "vida privada".

Sampaio (1998, p. 55) cita como primeiro antecedente do direito à privacidade um trabalho denominado "*Grundzuge des natrurrechts",* de David Augusto, em 1846, no qual o autor define como ato violador do direito à privacidade: incomodar alguém com perguntas indiscretas ou entrar em um aposento sem se fazer anunciar. O segundo antecedente, citado por Sampaio (1998, p.

55), foi o caso Affaire Rachel c. O'Connell[3], que trata o episódio ocorrido com uma famosa atriz do teatro clássico francês, do século XIX, que fora fotografada, a seu pedido, no leito de morte.

Ocorre que, de forma não autorizada, os fotógrafos disponibilizaram a sua imagem para elaboração de um desenho que foi posteriormente publicado no seminário *L'Illustration.* A família da atriz ajuizou ação em face do desenhista e o Tribunal Civil de Sena proferiu sentença no sentido de que não seria dado a ninguém reproduzir e dar publicidade a traços de uma pessoa em seu leito de morte, sem autorização formal da família.

Não obstante todos os antecedentes citados pela doutrina sobre a origem do direito à privacidade, considera-se marco inaugural da formulação do direito à intimidade e à vida privada foi o artigo de Samuel D, Warren e Louis D. Brandeis[4], publicada na *Harvard Law Review*, em 15 de dezembro de 1890.

O artigo de Warren e Brandeis teve como finalidade estabelecer limites para intromissão na vida privada, tendo em vista que Warren foi vítima de escândalo sobre sua vida conjugal, já que havia se casado com a filha de um senador, de origem bastante tradicional em Boston, levando uma vida dispendiosa e desordenada (NOJIRI, 2005, p. 100).

Nesse sentido, no célebre trabalho de Warren e Brandeis, os autores definiram apenas estritamente o *right to privacy,* limitando-se, tão somente a definir como um "direito a ser deixado só". Com isso, a privacidade passa a ser prerrogativa de uma emergente classe burguesa, com componente fortemente

[3] Caso julgado pelo Tribunal Civil de Sena, em 1958, no qual retrata o caso de Raquel, uma atriz famosa do teatro clássico francês do século XIX, tendo morte prematura aos 38 anos de idade, vitima de tuberculose. A irmã de Raquel, consternada com seu falecimento e para atender ao último pedido de sua irmã, contratou dois fotógrafos para reproduzir o seu retrato em seu leito de morte, mas o retrato não poderia ser reproduzido por qualquer outro motivo. (SAMPAIO, 1988, 55).

[4] Disponível em: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html. Acessado em: 27 de junho de 2014.

individualista, possibilitando que a burguesia se isolasse dentro de sua própria classe.

O trabalho de Warren e Brandeis foi considerado o antecedente de maior importância na abordagem do direito à privacidade. Sua publicação se deu no momento em que a América estava em transformação, marcada pelo início das grandes concentrações urbanas, pelo crescimento da migração, pelo desenvolvimento da imprensa, pela emancipação da mulher e pela industrialização. Diante destas transformações estavam criadas as condições para a invasão da privacidade.

Insta observar que esta definição da "*privacy"* analisa apenas um dos aspectos da privacidade e, por isso se torna muito perigosa a sua utilização nos dias de hoje, haja vista a complexa multiplicidade de situações existenciais.

Rodotá (2008, p. 28) entende que é importante esclarecer as inspirações que motivaram os "fundadores" da privacidade e os conduziram ao delineamento jurídico que propuseram àquela época. Warren era um conservador tradicional, interessava-se somente nos privilégios da alta burguesia, encarando com ressentimento a ação da imprensa à caça de escândalos políticos. Já Brandeis era liberal-progressista, ainda que preocupado com a privacidade das pessoas de maior projeção (intelectuais e artistas) e com os danos que poderiam lhes sobrevir pelas indiscrições jornalísticas.

Nessa perspectiva, o isolamento era privilégio de uma minoria eleita ou daqueles, que por opção ou necessidade viviam longe da comunidade (RODOTÁ, 2008, p. 26). Assim, a privacidade configurava-se como uma possibilidade da classe burguesa, devido às transformações socioeconômicas referentes à Revolução Industrial.

Locke (2005, p. 92-95), pensador mais fortemente associado à gênese do liberalismo, entendia que a sociedade de então estruturava-se em torno do binômio liberdade-propriedade.

Para Locke, o individualismo estrutura-se como um "individualismo possessivo", no qual a liberdade humana encontra seu fundamento na propriedade privada. Assim, a propriedade iria potencializar os direitos fundamentais do homem, incluindo a privacidade.

Nesse contexto, pode-se afirmar que no século XIX, a propriedade era concebida como essencial ao desenvolvimento da personalidade do indivíduo e que o direito de propriedade era condição indispensável para se chegar à privacidade. Assim, necessário se fazia uma mudança do eixo de gravitação da ordem jurídica, dissociando a propriedade da privacidade.

Todavia, esta não é a perspectiva nos dias de hoje sobre os direitos da personalidade. Assim, Doneda (2006, 115) adverte sobre a importância de atualmente, não construirmos o discurso sobre a privacidade a partir de bases proprietárias, através de uma relação com o espaço, a exclusão e com situações subjetivas patrimoniais, isto porque muitas vezes, tratar da esfera privada, significa, em princípio, um discurso baseado na exclusão, o que não mais se admite atualmente.

Nesse sentido, Doneda esclarece ainda que:

> a cumplicidade entre a proteção da privacidade e a da propriedade, não obstante, tenha então inicio, e assume diversas conotações dependendo do momento e do ponto de vista assumido: se é o da exclusão, o da dicotomia entre situações subjetivas patrimoniais e não patrimoniais, do direito subjetivo, da exploração econômica ou da eficiência (DONEDA, 2006, p. 116)

Para constatar a correlação da proteção da privacidade com a propriedade, pode-se mencionar, como exemplos: a base da elaboração jurisprudencial das regras de proteção da privacidade nos países da *common law* e a proteção da propriedade privada. No caso brasileiro, percebe-se que todas as Constituições desde a de 1824, previram expressamente a inviolabilidade de domicílio e da

correspondência, como forma de tutelar a privacidade[5]. Assim, pode-se afirmar que o nascimento da privacidade não se apresenta como a realização de uma exigência "natural" de cada indivíduo, mas como a aquisição de um privilégio por parte de um grupo (RODOTÁ, 2008, p.. 27).

Neste sentido, os instrumentos jurídicos de tutela foram modelados com base na propriedade, característica do direito burguês. Assim, exigências análogas àquelas que a burguesia fez valer ou não foram reconhecidas à classe operária ou o foram somente mais tarde, através de instrumentos jurídicos, como a tutela da personalidade nas fábricas.

Rodotá (2008, p. 27) acrescenta que foram as condições materiais de vida que acabaram por excluir a privacidade da classe operária. Como exemplo, vale lembrar os dados coletados por Engels sobre a situação habitacional dos operários ingleses em Londres, para perceber as conotações elitistas de privacidade.

Todavia, entende-se que a privacidade não pode ser considerada como uma noção unificadora, exprimindo exigências uniformemente difundidas na coletividade, isto porque, também seria equivocado considerar a privacidade de forma monolítica em relação à própria classe burguesa. Rodotá (2008, p. 28) adverte que a privacidade destina-se a desaparecer onde se degradam as condições de vida dessa classe, como ocorre com a pequena burguesia europeia confinada em habitações populares, na periferia de grandes cidades.

Assim, pode-se afirmar que a privacidade só passou a ser objeto de reflexão em razão das transformações sociais e tecnológicas, considerando-se que a afronta a este direito tem sido proporcional aos avanços tecnológicos e ao desenvolvimento cada

[5] Veja-se como na Constituição de 1824, no seu art. 179, VII já se tutelava a inviolabilidade de domicilio: "Todo o cidadão tem em sua casa asylo inviolável. De noite não se poderá entrar nella, senão por seu consentimento, ou para o defender de incêndio, ou inundação; e de dia só será franqueada a sua entrada nos casos, e pela maneira, que a lei determinar". Disponível em: http://planalto.gov.br/ccivil_03/constituicao/constituicao24.htm. Acesso em: 30 de jun. 2014.

vez mais assustador dos meios de comunicação. Nesse sentido, vale mencionar os danos causados à privacidade e intimidade da pessoa, quando as suas informações pessoais são transmitidas a terceiros sem o conhecimento e autorização do seu titular.

Veja-se a título de exemplo, a situação vivenciada por moradores de grandes cidades, que dispõem do programa do Google Earth, onde é possível verificar pessoas no movimento de suas atividades rotineiras, ou ainda, teor de mensagens, imagens que são reproduzidas sem o conhecimento do seu remetente.

Defende-se desta forma, que o direito à privacidade não sujeita o individuo apenas a uma posição passiva, mas também permite que a pessoa seja a condutora da construção e consolidação da sua esfera privada. Assim, na próxima seção analisar-se-á a privacidade, em um novo contexto, fazendo-se a devida correlação com o desenvolvimento tecnológico.

1.4 O mundo tecnológico e o conceito contemporâneo de privacidade

Sabe-se que o desenvolvimento tecnológico trouxe muitos benefícios para a sociedade, como a criação e ampliação do uso da *internet*, favorecendo os processos de comunicação, circulação de informações e de riquezas. Inobstante, o advento de novas dimensões de coleta e tratamento de informações pessoais, ampliaram os riscos de lesão à privacidade.

O debate acerca da privacidade não se restringe mais ao tema clássico da defesa da esfera privada contra as invasões externas, isto porque tal discussão evoluiu qualitativamente, o que nos faz considerar que os problemas da privacidade no âmbito da infraestrutura da informação representa um dos componentes mais importantes atualmente.

Assim, parece cada vez mais insuficiente a definição de privacidade como “o direito a ser deixado só”, que abriu espaço para uma noção cujo centro de gravidade é a possibilidade de cada

um controlar o uso das informações que lhe dizem respeito, não significando que este último aspecto estivesse ausente nas definições tradicionais, entretanto, servia muito mais para exaltar o caráter individualista, apresentando a privacidade como mero instrumento para ser deixado só.

Hodiernamente, chama-se a atenção para a possibilidade de indivíduos e grupos controlarem o exercício dos poderes baseados na disponibilização de informações, é o chamado direito à autodeterminação informativa, ou seja, o poder de controlar as suas próprias informações.

Para se analisar o direito à autodeterminação informativa, faz-se necessário tecer algumas considerações acerca da noção de liberdade para Kant (1980), que a entendia dotada de um sentido negativo e um sentido positivo. No primeiro sentido, como sendo liberdade de escolha, independência do ser para fazer suas próprias escolhas. Segundo Kant, o arbítrio humano seria uma escolha que, embora possa ser realmente afetada por impulsos, por eles não pode ser determinada, o que significa dizer que liberdade é a não intromissão, não impedimento, ou seja, ter liberdade é não sofrer interferência dos outros.

No sentido positivo, Kant (1980) entendia a liberdade como sendo a autonomia da vontade, a faculdade de se dar a si mesmo, ou a sua liberdade uma lei. Em outras palavras, a liberdade para ele é a autonomia da pessoa, de fazer a sua vida e as suas decisões dependerem só de si mesmo, e não de forças externas.

Acerca do conceito de liberdade, Pianovski (2009, p. 14) esclarece que, muito embora se verifique entre os liberais uma prevalência de noções que remetem o conceito de liberdade a uma ausência de coerção, sobretudo nas relações privadas, qualificando-se como liberdade negativa, há desde compreensões que trazem à liberdade um sentido de autodeterminação inerente ao que se pode denominar de liberdade positiva, até posições que sustentam uma concepção francamente substancial de liberdade.

Nesse contexto, a autodeterminação informativa é apenas um dos aspectos do direito à privacidade, se refere especificamente à proteção dos dados pessoais, concedendo ao indivíduo o direito de controlar as suas informações pessoais que estejam em poder tanto de arquivos públicos, como de arquivos privados.

Assim, pode-se afirmar que o direito à privacidade se mostra como uma nova forma de liberdade pessoal, que já não é mais a liberdade negativa de recusar ou proibir a utilização das informações sobre a própria pessoa. Transformou-se em liberdade positiva de poder controlar os dados concernentes à própria pessoa (SAMPAIO, 1998, p. 492-493).

Rodotá (2008, p. 32) lembra que a quantidade de informações coletadas por instituições públicas e privadas tem em vista dois objetivos: a aquisição de elementos necessários à preparação de programas de intervenção social pelos poderes públicos e, o desenvolvimento de estratégias empresariais privadas. Para os fins deste trabalho, será analisada de forma aprofundada tão somente a tutela da privacidade em relação a agentes privados, fazendo-se apenas algumas considerações à proteção de dados pessoais coletados por entes públicos.

De toda sorte, é necessário informar que a defesa da privacidade assume significados diversos, dependendo do objetivo perseguido com a coleta de informações. No que toca à coleta de informações por entes públicos para os fins de Estado, como é o caso aqui no Brasil, das pesquisas elaboradas pelo Instituto Brasileiro de Geografia e Estatística – IBGE, sua tutela é específica. Há todavia, uma certa resistência em fornecer determinadas informações, sobretudo a classe média. O que dificulta a elaboração de políticas públicas sérias, cuja estruturação requer um profundo conhecimento das situações reais.

Nessa perspectiva, Rodotá (2008, p. 29) recorda que durante os censos, na Itália, houve reações contra algumas perguntas contidas no formulário do recenseamento, o que foi tranquilizado assim que o ISTAT (*Istituto Nazionale di Statística*) assegurou que

nenhum dos dados coletados seria transmitido a outros órgãos públicos (principalmente àqueles fiscais).

Na verdade, a coleta de dados utilizados pelos poderes públicos com o objetivo de implementar uma política pública séria e consistente não parece ser perigosa para a privacidade, considerando que para esses dados não haveria necessidade de controles especiais ou reconhecimento de um direito de acesso.

Todavia, Rodotá (2008, 32) adverte novamente que os dados coletados anonimamente podem ser manipulados de forma lesiva aos direitos do indivíduo, citando como exemplos, os dados que digam respeito a uma minoria racial; ou às consequências de uma decisão política ou econômica tomada com base na análise dos dados anônimos. Nesse sentido, entende-se que excluir o direito de acesso aos dados anônimos significa permanecer preso à velha lógica individualista, recusando-se a aproveitar a oportunidade oferecida pelo uso da internet para promover uma expansão das possibilidades de intervenção e de participação dos indivíduos e dos grupos.

Rodotá (2008, p. 33) esclarece que continuar a excluir formas generalizadas de acesso a tais informações significa não apenas deixar nas mãos de grupos privilegiados o poder de tomar decisões, mas, sobretudo, impedir a quem não esteja no "círculo mágico" de poder, a possibilidade de criticar tempestivamente as escolhas governamentais e propor alternativas.

A socialização das informações se mostra como indispensável para se colocar em plano de igualdade todos aqueles que estão interessados em contribuir, por meio da livre discussão, para determinação de política pública adequada ao seu país, desfrutando, assim, das possibilidades de avaliação dos dados disponíveis.

Feitas estas considerações acerca de uma das possibilidades de tutela da privacidade no que diz respeito a dados pessoais coletados por órgãos públicos, passa-se a analisar a tutela da privacidade na perspectiva do tratamento ou manipulação de dados

por órgãos privados, o que Rodotá (2008, p. 28) chama de "desenvolvimento de estratégias empresariais privadas".

Sabe-se que a globalização e os avanços tecnológicos trouxeram muitas consequências para a sociedade, tanto do ponto de vista da facilidade do acesso à socialização das informações, como também da dificuldade do controle sobre essas informações, inclusive, aquelas de cunho pessoal. A informação tem um importante papel como ponto de partida para uma série de situações jurídicas, tendo em vista a sua visibilidade pela sociedade pós industrial.

Os problemas da privacidade, observa Rodotá (2008, 35), devem ser analisados numa dimensão que leve em conta a existência de uma profunda revisão dos critérios de classificação das informações pessoais, segundo uma escala de valores renovada, na qual deveria ser garantido o máximo de proteção às informações suscetíveis de originar práticas discriminatórias, como as que dizem respeito às opções políticas, religiosas e sexuais.

A caracterização da nossa sociedade como uma organização cada vez mais baseada na circulação de informações, denominada sociedade de informação, comporta o surgimento de um novo recurso de base, ao qual se coliga o estabelecimento de novas formas de poder. Entretanto, há de se perquirir como se dá a legitimação deste poder.

Esse processo de legitimação de poder se desenvolve, segundo Rodotá (2008, p. 35) ao longo de um caminho que vai da demonstração da impossibilidade do Estado e da indústria em renunciar a uma infraestrutura normativa cada vez mais ampla e sofisticada, chegando a alcançar a promessa de uma garantia efetiva.

Nos dias atuais, torna-se cada vez mais difícil identificar os tipos de informações acerca das quais o cidadão estaria disposto a divulgar completamente, renunciando definitivamente ao controle das modalidades de seu tratamento e atividade dos sujeitos que as utilizam. Assim, percebe-se que até as informações mais banais podem, se integradas a outras, provocar danos à pessoa interessada.

É importante ressaltar que publicidade e controle não são termos contraditórios, como publicidade e sigilo. O que se defende é a possibilidade de controle destas informações por seu titular, onde se admitir a máxima circulação das informações de conteúdo econômico, por exemplo, deve-se permitir um real poder de controle aos interessados, não só sobre a exatidão dessas informações, mas também sobre os sujeitos que as operam e as modalidades da sua utilização.

Segundo Leonardi, "a adoção do segredo como elemento essencial da privacidade limita demais o conceito". O referido autor arremata, afirmando que:

> {...} Além de não existir relação direta entre segredo e privacidade - há informações secretas que não são privadas, tais como planos militares e assuntos privados que não são secretos, tal como a relação de débitos de alguém – a privacidade engloba mais do que o impedimento da revelação de informações secretas. Entre outros elementos, a privacidade inclui a possibilidade de o individuo autorizar a divulgação de informações a seu respeito do modo que desejar (LEONARDI, 2012, p. 66).

Nessa perspectiva, os cidadãos têm o direito de exercer um controle direto sobre aqueles sujeitos que manipulam informações fornecidas, atribuindo-lhes uma espécie de *plus* poder. Entretanto, sabe-se que raramente o cidadão perceberá o sentido que a coleta de dados poderá assumir, quando utilizados por uma organização complexa e dotada de meios sofisticados para o tratamento destes dados. Sem considerar que a relação entre o indivíduo isolado e as grandes organizações de coleta de dados é absolutamente assimétrica, fazendo com que o controle por parte do titular das informações pareça algo ilusório.

Todavia, a dificuldade em se concretizar esse controle não pode servir de óbice à tutela da privacidade. Conforme seu novo significado, já analisado anteriormente, a privacidade também

corresponde ao direito de manter o controle sobre suas próprias informações, a chamada autodeterminação informativa.

A esse respeito, é necessário observar que o conteúdo dos termos "informação" e "dados" se sobrepõe em várias oportunidades, o que justifica uma certa interpenetração, isto porque ambas as expressões servem para representar um fato da realidade. No entanto, Doneda entende que, embora o conteúdo dos vocábulos se sobreponha a várias ocasiões, cada um carrega um peso particular a ser considerado (DONEDA, 2006, p. 152).

A União Europeia, por intermédio da Diretiva do Parlamento Europeu e do Conselho 95/46/CE, definiu dados pessoais, no seu art. 2º, como qualquer informação relativa a uma pessoa singular identificada ou identificável; sendo identificável aquela pessoa que possa ser identificada, direta ou indiretamente, por referência a um número de identificação ou a algum elemento específico da sua identidade física, psíquica, econômica ou social.

Dado pessoal pode ser definido como dado relacionado a um individuo identificado ou identificável, independente do tipo de registro, se por escrito, imagem ou som. Identificado é o indivíduo que já é conhecido; e identificável é a pessoa que pode ser conhecida diretamente pelo próprio possuidor de seus dados, ou indiretamente através de recursos e meios à disposição de terceiros (CASTRO, 2005, p. 70-71).

Assim, surge a figura do banco de dados, que consiste em um conjunto de informações organizadas, com ou sem uso da informática, segundo uma determinada lógica. O uso informatizado do banco de dados pode armazenar um grande volume de informações, agrega-las e combiná-las em uma multiplicidade de modos e um curto espaço de tempo se comparado ao tratamento realizado por um banco de dados manual (DONEDA, 2006, p. 158).

Com o desenvolvimento da tecnologia, surgiu a necessidade de se compreender diretamente os dados pessoais, em situações em que não estão necessariamente ligados a um banco de dados,

isto porque uma informação pode ser transmitida a determinado destinatário, sem no entanto, vincular-se a um banco de dados, como por exemplo, quando se transmite uma mensagem contendo dados do remetente a um destinatário que posteriormente a transmite a terceiros. Dessa forma, verificou-se que o conceito de banco de dados perdeu a centralidade nesta matéria, que passou a entender que mais importante, eram os dados pessoais em si, particularmente considerados.

A informação pessoal, conforme observa Doneda (2006, p. 159) "pode ser agrupada em subcategorias, ligadas a determinado aspecto da vida de uma pessoa". Assim, uma determinada classificação pode ser pressuposto para a qualificação das normas a ser aplicadas a algumas categorias de dados pessoais, como acontece com as normas sobre as movimentações bancárias de uma pessoa, que seriam enquadradas no chamado sigilo bancário.

Insta destacar uma categoria específica de dados, chamados sensíveis, que significam determinados tipos de informação, que caso sejam conhecidos ou divulgados, poderiam se prestar a uma potencial utilização discriminatória, como aqueles que dizem respeito a orientações políticas, religiosas, filosóficas, sexuais, raciais e outros.

Para Rodotá (1995, p. 85) os dados sensíveis são frutos de uma observação pragmática da diferença que apresentam e do efeito do tratamento destes dados em relação aos demais. Não raro, empregadores se valem de dados pessoais sensíveis, no ato da seleção de uma vaga de emprego, para descobrirem informações do tipo orientação sexual, religiosa, racial, como condição para admissão, caracterizando posição absolutamente discriminatória.

Nesse sentido, é importante ressaltar que hoje não é mais possível se conceber a privacidade de maneira tão reducionista, restringindo a sua definição a um "direito de ser deixado só". Nessa perspectiva, Rodotá recorda que:

> não é possível considerar os problemas da privacidade somente por meio de um pêndulo entre "recolhimento" e "divulgação"; entre o homem prisioneiro de seus segredos e o homem que nada tem a esconder; entre a "casa-fortaleza, que glorifica a privacidade e favorece o egocentrismo, e a "casa-vitrine", que privilegia as trocas sociais; e assim por diante (RODOTÀ, 2008, p. 25).

Analisar a privacidade segundo essas perspectivas são alternativas cada vez mais abstratas, considerando que nelas se reflete uma forma de encarar a privacidade por uma dimensão absolutamente individualista, como sempre esteve confinada por conta de sua origem, no entanto, nos dias atuais, fala-se em outras facetas da privacidade, como por exemplo, o direito de proteção jurídica do corpo. Nesse sentido, Konder (2013, p.07) exemplifica tal hipótese com os atos de disposição permanente, como a amputação de um membro, que é vedado por lei, por traduzir a ideia de retirada do padrão natural do corpo. É o caso dos denominados *Wannabes* ou *amputees-by-choice*[6].

Por esta razão é que se afirma que o nascimento da privacidade está historicamente associado à desagregação da sociedade feudal, em que os indivíduos eram ligados por uma série de relações que se refletiam na própria organização de sua vida cotidiana, sendo o isolamento privilégio de poucos eleitos ou daqueles que por necessidade ou opção viviam distantes da comunidade.

De fato, uma definição de privacidade nos moldes tradicionais, como sendo "o direito a ser deixado só" está cada vez mais ultrapassada, ainda que continue a abranger um aspecto importante do problema, isto porque numa sociedade de informação devem prevalecer definições funcionais de privacidade, fazendo-se referência à possibilidade de um sujeito conhecer,

[6] São pessoas movidas por um profundo desejo de adequar seu corpo a uma visão própria de identidade, buscam voluntariamente a amputação de um membro, mas impedidas pelas restrições legais e regulamentares, muitas vezes recorrem a um mercado negro de amputações, causando sérios riscos à sua saúde (KONDER, 2003, p. 6173).

controlar, endereçar, interromper o fluxo das informações a ele relacionadas (RODOTÁ, 2008, p. 92).

A sociedade hoje é mais intrusiva do que em outros momentos da história. A indústria da informação, a imprensa moderna e os governos estão cada vez mais intrusivos, na opinião de Mills (2008, p. 146), em que cada um deles deve ter motivações para invadir a privacidade pessoal. O fato é que as pessoas estão correndo riscos.

O referido autor questiona se as pessoas estão compreendendo o vasto âmbito de intromissão e os potenciais efeitos desta invasão. Como exemplo, o Estado, com a finalidade de garantir a segurança para os cidadãos, instala câmaras guardiãs para o controle e tentativa de redução dos níveis de violência, no entanto, os controladores destes equipamentos o utilizam de maneira indevida, na medida em que se aproveitam das suas funções para invadir a privacidade das pessoas, especialmente mulheres.

Dessa forma, a privacidade individual é o cerne da identidade e liberdade pessoal, isto porque quando alguém se torna membro da sociedade concorda em ceder um pouco de liberdade e independência. Essa liberdade que permanece é o que constitui a noção comum da privacidade individual. No entanto, um desafio limiar é formular uma definição abrangente de privacidade (MILLS, 2008, p. 147).

Pode-se perceber que uma ampliação progressiva da noção de esfera privada, que compreende agora situações e interesses antes excluídos de proteção jurídica e que se projeta muito além da mera identificação de um sujeito e seus comportamentos.

Nesse sentido, Rodotà (2008, p. 92) diferencia a esfera privada da privacidade. A esfera privada pode ser definida como "aquele conjunto e ações, comportamentos, opiniões, preferências, informações pessoais, sobre os quais o interessado pretende manter um controle exclusivo". Por outro lado, privacidade pode ser identificada "com a tutela das escolhas de vida contra toda forma de controle público e de estigmatização social".

Dessa forma, percebe-se uma redefinição no conceito de privacidade, que além do tradicional poder de exclusão, no direito de estar só, atribui um leque cada vez mais amplo de situações, em que a privacidade possa estar ameaçada, e consequentemente ampliando a possibilidade de poder de controle. Como bem ensina Rodotà (2008, p. 93), "privado aqui significa pessoal e não necessariamente secreto".

Pode-se afirmar que a sequência hoje mais adequada é "pessoa-informação-circulação-controle" e não mais "pessoa-informação-sigilo", em torno do qual foi construído o conceito clássico de privacidade, tendo o titular desse direito o poder de exigir formas de circulação controlada (RODOTÀ, 2008, p. 93).

Insta observar que a tecnologia contribuiu para a reengenharia dessa esfera privada, na medida em que reduziu a necessidade dos contatos sociais cotidianos, favorecendo as compras à distância, a realização de transações bancárias, as videoconferências, etc.

A tecnologia contribuiu para moldar uma esfera privada mais rica, na opinião de Rodotà (2008, p. 95), porém mais frágil, isto porque cada vez mais exposta a ameaças, violações, principalmente no que concerne à privacidade. Daí a necessidade do fortalecimento da proteção jurídica, da ampliação das formas de controle, pois a importância atribuída à circulação e ao controle das informações não pode negligenciar os aspectos clássicos do sigilo e da proteção de dados pessoais como características fundamentais do direito à privacidade.

Nesse sentido, verifica-se uma tendência de se inserir o direito à privacidade entre os instrumentos de tutela da personalidade, desvinculando-o do direito de propriedade como originariamente foi concebido. Há, igualmente a necessidade premente de se conceder uma tutela integral à personalidade, que reforça a tendência de sistematização global da privacidade, apta a cotejar as possíveis lesões derivadas do manejo de bancos de dados públicos e privados, arquivos eletrônicos e outros.

A necessidade de limitação geral à ação dos bancos de dados é uma exigência para que seja efetivada a tutela da privacidade. Na União Europeia, estas limitações encontram-se em uma série de princípios presentes na primeira e segunda geração de leis sobre tutela das informações, preceitos estes que serão analisados mais adiante.

No Brasil, somente recentemente, foi aprovada e sancionada uma lei específica para proteção dos dados pessoais, Lei 13.709/2018, a denominada Lei Geral de Proteção de Dados Pessoais. Até agosto de 2018, só havia uma legislação genérica que não tutelava todos os aspectos da proteção de informações pessoais, como por exemplo, a lei do *Habeas Data,* que permite apenas o conhecimento de informações a respeito do interessado, bem como a sua retificação, se for o caso.

Tramitavam na Câmara dos Deputados três projetos de leis acerca da proteção de dados pessoais. Um deles foi apresentado pelo governo, ainda na época da ex-presidente Dilma Rousseff, e exigia que os dados só poderiam ser usados e manipulados mediante autorização, além de estabelecer uma série de restrições em relação a informações consideradas sensíveis, como opção sexual e posição política, e cria uma agência reguladora para fiscalizar o setor (PL 5276/16). O outro, de autoria do deputado Milton Monti (PR-SP) considera legítimo o interesse de quem quiser manusear os dados e sugere a auto-regulamentação do setor no lugar de um órgão regulador centralizado, a exemplo do que acontece hoje com a publicidade (PL 4.060/12), que se transformou na Lei 13.709/18. E um terceiro projeto (PL 6291/16) que alterou o Marco Civil da Internet (Lei 12.965/14) para deixar clara a proibição do compartilhamento de dados pessoais dos assinantes de aplicações de internet.

O novo panorama tecnológico e as suas transformações se apresentam como sendo a via que deve ser percorrida para se chegar à plena compreensão dos efeitos sociais das tecnologias da

informação e da comunicação. Nessa perspectiva, Rodotá sintetiza esses efeitos com referência à privacidade da seguinte forma:

> - Passamos de um mundo no qual as informações pessoais estavam substancialmente sob exclusivo controle dos interessados para um mundo de informações divididas com uma pluralidade de sujeitos;
> - passamos de um mundo no qual a cessão das informações era, em grande parte dos casos, efeito de relações interpessoais, tanto que a forma corrente de violação da privacidade era a "fofoca", para um mundo no qual a coleta das informações ocorre através de transações abstratas;
> - passamos de um mundo no qual o único problema era o do controle do fluxo das informações que saíam de dentro da esfera privada em direção ao exterior, para um mundo no qual se torna cada vez mais importante o controle das informações que entram, como demonstra a crescente importância assumida pelo direito de não saber, pela atribuição aos indivíduos do poder de recusar interferências em sua esfera privada, como as derivadas da remessa de material publicitário e do marketing direto (RODOTÀ, 2008, p. 127-128)

As tecnologias da informação e da comunicação contribuíram para tornar cada vez mais sutil a relação entre a esfera pública e a esfera privada, possibilitando a construção livre da esfera privada e do desenvolvimento autônomo da personalidade como condições para determinar a efetividade e a amplitude da liberdade na esfera pública.

Da análise dos efeitos sociais das tecnologias de informação e comunicação citados acima por Rodotà (2008), pode-se depreender que a evolução destas tecnologias tomou proporções inimagináveis, fazendo com que o controle fique cada vez mais difícil, distante da

realidade, todavia, esta dificuldade não pode ser considerada como óbice para que os sujeitos utilizem poderes diretos de controle, determinando uma maior transparência da esfera dos coletores de informações, sejam agentes públicos ou privados.

Outra questão que merece relevo na seara da privacidade, diz respeito às informações relativas a opiniões políticas ou sindicais, consideradas como "núcleo duro" da privacidade, por Rodotá (2008, p. 129).

O problema que esta questão levanta é o fato de tais informações serem utilizadas para fins discriminatórios, o que constantemente é visto por parte de empregadores, antes mesmo da contratação, levando muitas vezes o indivíduo a perder a chance de um bom emprego, por questões absolutamente discriminatórias, como foi dito anteriormente.

Assim, surge um verdadeiro paradoxo: se o melhor é alocar este tipo de informação na esfera privada, com total controle por parte do seu titular; ou alocá-lo logo na esfera pública, como manifestação do seu direito à liberdade de expressão, também tutelado constitucionalmente. Nesse sentido, Rodotá (2008, p. 129) entende que "altera-se assim, profundamente, a função sócio política da privacidade, que se projeta para além da esfera privada, para se tornar elemento constitutivo da cidadania".

A tutela das informações pessoais revela-se como elemento essencial da personalidade e da cidadania, e por isso necessita-se que a sociedade da informação evolua para uma sociedade do conhecimento e do saber, e não para uma sociedade de vigilância, de classificação (RODOTÁ, 2008, p. 137).

Nesse contexto, observa-se que o controle das informações pessoais é a parte menos desenvolvida da privacidade, conforme analisa Mill (2008, p. 171), ou seja, a esfera de menor proteção legal, isto porque as pessoas procuram proteger as suas informações, tanto no momento de disponibilizá-las, como quando houver uma liberação indevida, causando alguma espécie de dano ao seu titular.

Em diversos países, percebe-se que as regras para a coleta e circulação de informações se fundamentam no consentimento livre e informado do interessado, não bastando que o sujeito tenha dado seu consentimento, necessário se faz saber se tal consentimento foi adequado ou mesmo manifestado de forma livre. Assim, verifica-se em muitas relações, uma assimetria de poder entre os sujeitos, na qual a figura do contratante é vulnerável e merece maior proteção.

Quando se analisa o sistema norte-americano, por exemplo, percebe-se que do consentimento para a coleta de informações sobre a saúde depende a própria possibilidade de ser curado. Nesse caso, se continua a falar do consentimento informado como instrumento posto à disposição do individuo para tutelar a sua esfera privada (RODOTÁ, 2008, p. 138).

Nesse caso, Rodotá (2008, p. 138) adverte que só restam dois caminhos para se tutelar a privacidade: o de manter, sempre que possível, o princípio da cobertura pública das despesas médicas, eliminando pela raiz, o estímulo à demanda de informações sensíveis; ou então, tornar indisponíveis as informações sobre a saúde, partindo da premissa de que a saúde é direito fundamental e que não se pode obrigar uma pessoa a ceder dados que sejam de aspectos particulares da sua personalidade.

Nessa perspectiva, pode-se afirmar que a tutela da privacidade manifesta-se por meio de múltiplos instrumentos, que não são incompatíveis entre si e que, ao menos em algumas situações, podem funcionar em conjunto.

Leonardi (2012, p. 68-69) lembra que as preocupações relativas à criação, manutenção e acesso a banco de dados eletrônicos e cadastros informatizados não são novas e cita fato ocorrido no governo norte-americano, em 1973, em que o governo norte-americano divulgou um relatório intitulado *Records,*

computers and right of citizen, abordando essas questões e sugerindo a adoção de um código de melhores práticas[7].

Percebe-se que já naquela época havia a preocupação com a proteção dos dados pessoais, o que fez Rodotá (1973, p. 14) observar que o que originou a transformação da informação foi o surgimento dos computadores.

No Brasil, a Constituição Federal de 1988 dispõe acerca do sigilo de dados de forma um tanto genérica, estabelecendo no art. 5º, XII que:

> é inviolável o sigilo de correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (BRASIL, 1988).

Percebe-se que o direito à inviolabilidade do sigilo de dados não se refere aos dados em si, mas à restrição quanto à sua utilização. A transmissão de informações é que não pode ser violada por sujeito estranho à comunicação (FERRAZ JUNIOR, 1993, p. 82). Todavia, como já fora exposto, no Brasil não há uma lei específica de proteção dos dados pessoais, há tão somente projetos de leis em tramitação na Câmara dos Deputados.

Schneier (2006) utilizou a metáfora do "maremoto" de dados pessoais gerados nas relações do cotidiano para explicar a poluição da era da informática. Em sua comparação, o autor diz que se a produção industrial gera resíduos, computadores utilizados para processar informações geram dados, que se ignorados

[7] O referido código deveria possui cinco elementos essenciais: a) não deve haver sistemas de coleta e manutenção de dados cuja própria existência seja secreta; b) deve haver um meio de um individuo conhecer quais informações a seu respeito existem em um banco de dados e como elas são utilizadas; c) deve haver uma maneira de um individuo impedir que informações a seu respeito, obtidas para uma determinada finalidade, sejam disponibilizadas ou utilizadas para outra finalidade, sem o seu consentimento; d) deve haver um meio de um individuo corrigir um registro de informações a seu respeito; e) qualquer organização que crie, mantenha, utilize ou dissemine registros de dados pessoais que permitam a identificação de alguém deve assegurar a confiabilidade dos dados para o seu uso previsto e deve tomar as precauções para impedir o mau uso dos dados. (LEONARDI, 2012, p. 68-69).

permanecerão registrados para sempre, consequentemente sendo necessário regular sua geração, uso e seu descarte.

Dessa forma, constata-se que a complexa rede de informações, especialmente sobre dados pessoais, constitui ameaça à privacidade. Há um flagrante perigo à intimidade a disseminação deste amplo sistema de informações computadorizadas.

A ideia de privacidade como proteção de dados pessoais, observa Leonardi (2012, p. 69), encontrou eco após a lei alemã do censo de 1983, que determinava o recenseamento geral da população, coletando-se dados referentes ao domicílio, profissão e renda dos indivíduos. Tais informações tinham como objetivos: reunir dados estatísticos, tais como crescimento populacional e densidade demográfica e compará-los com dados armazenados em registros públicos.

Entretanto, o Tribunal Constitucional Alemão[9] declarou a nulidade dos dispositivos legais que previam a comparação e a transmissão de dados coletados para repartições públicas. Este Tribunal reconheceu pela primeira vez, a existência de um direito à autodeterminação informativa, entendendo-se como direito de um indivíduo se proteger contra a coleta, o armazenamento, o uso e a revelação de seus dados (LEONARDI, 2012, p. 69-70).

No entanto, se mostra como incontestável a importância dos bancos de dados e dos cadastros interligados por meio de internet para ampliação da circulação de produtos e serviços e diminuição dos riscos e dos custos da atividade econômica. O que na verdade se questiona é a falta de controle de tais informações pelo seu titular, podendo causar assim, um dano irreparável à pessoa humana.

A era da informação e das redes, na opinião de Leonardi (2012, p. 72), é marcada pelo anonimato dos agentes e pela complexidade e velocidade das relações comerciais, a troca de informações é instantânea e ocorre em uma escala sem precedentes. Isto se deve ao barateamento dos custos de armazenamento de informações e a facilidade de sua manipulação, provocando o surgimento de bancos de dados e cadastros de toda espécie.

Insta observar que dados são para sempre, o registro eletrônico não tem limitações, como antes do surgimento dos computadores, que os registros eram mais restritos, pois nem todos tinham acesso a tais informações, havia mais dificuldade na transmissão destes dados. Hoje, os computadores têm a possibilidade de coletar, armazenar, manipular, trocar e reter quantidades imensuráveis de informações (LEONARDI, 2012, p. 72).

Dessa forma, pode-se afirmar que a evolução tecnológica, com o surgimento dos computadores foi um divisor de águas no que se refere aos riscos ocasionados pela manipulação de dados pessoais, sem o conhecimento de seu titular. Antes do advento do computador, os dados eram coletados e armazenados em papel, sendo difícil de pesquisar e correlacionar; já os dados computadorizados podem ser pesquisados facilmente, podendo ser coletados, usados e abusados.

Assim, vê-se que o conceito de privacidade necessitava avançar e se afastar daquela definição tradicional como o "direito a ser deixado só", considerando que tal conceito não se aplica a determinadas situações, nas quais o objeto da privacidade não é o isolamento, e sim manter o controle das nossas próprias informações, a chamada autodeterminação informativa.

No entanto, Leonardi (2012, p. 78-79) entende que o conceito de privacidade, como o poder de controle de informações, revela-se muito vaga, isto porque não há uma explicação acerca dos tipos de informação que o indivíduo deve controlar. Observa também, que este conceito tem como objeto as informações e os dados sobre os quais o indivíduo quer exercer controle, mas entende que a privacidade não é simplesmente uma prerrogativa individual de caráter subjetivo, pois ela engloba aquilo que a sociedade considera apropriado proteger.

A inserção de informações pessoais em bancos de dados foi objeto de discussão pelo Superior Tribunal de Justiça (Resp.

22.337-RS)[8], no ano de 1995. Trata-se de cancelamento da inserção de dados pessoais constantes em bancos de dados de serviço de proteção ao crédito após o prazo de cinco anos. Na oportunidade, o relator Min. Ruy Rosado de Aguiar asseverou que

> A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações da vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa discriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos ou privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir ao Estado ou ao particular, para alcançar fins contrários à moral ou ao direito (REsp. 22.337/RS, 1995).

Percebe-se que já em 1995 o problema da inserção de informações pessoais em bancos de dados causava preocupação. No entanto, naquela época a preocupação se resumia aos bancos de dados de serviços de proteção ao crédito, restringindo-se a questão em saber se a inserção foi devida ou indevida.

Na análise sobre a proteção das informações pessoais, a Suprema Corte Americana manifestou o entendimento de que as informações são protegidas constitucionalmente e que a privacidade inclui não apenas o interesse na tomada de certas decisões importantes, mas também no interesse individual de evitar a revelação de assuntos pessoais (MILL, 2008, p. 171).

[8] BRASIL. Superior Tribunal de Justiça. RESP n° 22.337/RS. Recorrente: Clube de Diretores Lojistas de Passo Fundo-RS. Relator Min. Rui Rosado de Aguiar. Julgamento em 13/02/1995. Diário de Justiça em 20/03/1995. Disponível em: < http://stj.gov.br/SCON/jurisprudencia>. Acesso em 27 de jun. 2014.

Atualmente, o tema cresceu em importância, na medida em que a revolução tecnológica permitiu novas formas de inserção e manejo de informações pessoais que transcendem aos antigos bancos de dados de serviços de proteção ao crédito. Os bancos de dados colecionam verdadeiros "perfis" de pessoas, sem que as mesmas tenham ao menos conhecimento, culminando assim com uma afronta à privacidade da pessoa humana, tendo em vista que os dados pessoais representam a sua própria personalidade. O grande problema é que muitas vezes esse perfil destoa da realidade, passando a representar falsamente a pessoa.

Por esta razão é importante destacar que o direito à autodeterminação informativa, é apenas um dos aspectos em que se pode analisar hoje a privacidade, pois este seria um direito bem mais amplo, protegendo como se viu acima, a vida, o corpo, as crenças, os pensamentos e outros.

Quanto ao direito ao próprio corpo, por exemplo, Konder (2013, p. 361), lembra que o mecanismo que autorizou juridicamente as cirurgias de modificação de sexo foi o chamado paternalismo médico, ou seja, o legislador poderá abrir mão da naturalidade e da moralidade, em nome da voz mais forte da ciência. Em outras palavras, tanto a moralidade como a imoralidade passam a ser consentidas, se autorizadas pelo médico, enquadrando-se no critério da finalidade terapêutica.

O que se defende neste trabalho, é a possibilidade de o indivíduo, titular das informações, ter o seu absoluto controle, mesmo sabendo que há informações que não são estritamente privadas, como por exemplo, no caso de uma pessoa pública, que a imprensa noticia que está acometida de doença incurável.

Nesse sentido, se mostra como oportuna, a participação do legislador ordinário, no sentido de estabelecer limites ao controle dos dados pessoais, especificando que situações deveriam ser controladas pelo titular, e quais poderiam não sofrer tal controle.

Insta lembrar que o direito à privacidade não ostenta caráter absoluto, assim como todo direito fundamental e da personalidade,

podendo sofrer limitações, tais como: o interesse público, liberdade de expressão e de informação.

Nesse contexto, Dotti (1980, p. 141) ensina que em oposição ao direito a esta esfera privada, existem limitações, dentre elas: os interesses: da segurança nacional, da investigação criminal; da saúde pública; da história; da Administração Pública; da crônica policial, dentre outros.

Verifica-se então, que o direito à privacidade poderá entrar em rota de colisão com outro direito, também dito fundamental, é o que ocorre quando a privacidade entra em conflito com a liberdade de expressão e informação. Assim, como bem ensina Edilson Pereira de Farias (2000, p. 120), a solução para tal conflito deverá se basear nos fundamentos da colisão de princípios, não podendo haver incompatibilidade total entre os direitos, e sim concorrência entre eles.

Quando se trata de conflito entre princípios, Alexy destaca a necessidade de se fazer distinção entre princípios e regras que, apesar de não ser uma distinção nova, sente-se a ausência de clareza em algumas diferenças feitas pela doutrina. Para Alexy, há diversos critérios para se distinguir regras de princípios, afirmando que

> Provavelmente aquele que é utilizado com mais frequência é o da generalidade. Segundo esse critério, princípios são normas, com grau de generalidade relativamente alto, enquanto o grau de generalidade das regras é relativamente baixo. Um exemplo de norma de grau de generalidade relativamente alto é a norma que garante a liberdade de crença. De outro lado, uma norma de grau de generalidade relativamente baixo seria a norma que prevê que todo preso tem o direito de converter outros presos à sua crença (ALEXY, 2008, p. 87).

Vê-se que no primeiro exemplo citado por Alexy (2008, p. 89), pode-se classificar como princípio, e o segundo como regra. No entanto, o referido autor sustenta que são possíveis três teses acerca da distinção entre princípios e regras. A primeira defende

que toda tentativa de diferenciar as normas em duas classes: princípios e regras, seria fadada ao insucesso, isto porque pode acontecer de uma norma com alto grau de generalidade não ser aplicável de pronto.

Os defensores da segunda tese, embora aceitem a divisão entre regras e princípios, salientam que essa diferenciação é somente de grau, ou seja, levam em consideração apenas o critério da generalidade. Por fim, a terceira tese sustenta que entre regras e princípios não há apenas uma diferença de grau, mas também qualitativa.

Alexy (2008, p. 90) arremata afirmando que, "*princípios* são normas que ordenam que algo seja realizado na maior medida possível dentro das possibilidades jurídicas e fáticas existentes". Consequentemente, princípios são "mandamentos de otimização", que se caracterizam por poderem ser satisfeitos em graus variados e pelo fato de que a medida devida de sua satisfação não depende somente das possibilidades fáticas, mas também das possibilidades jurídicas.

Resta evidenciado que o direito à privacidade, como direito fundamental que é, tem natureza principiológica. Nesse caso, quando entra em conflito com outro direito dito fundamental, caracteriza uma colisão entre princípios, devendo ser solucionada pela ponderação, método que decide pela precedência de um princípio em relação a outro, não invalidando nenhum dos princípios conflitantes.

No próximo capítulo, para concluir as principais questões acerca do direito à privacidade, no que diz respeito à autodeterminação informativa do indivíduo, far-se-á uma análise para demonstrar a cumplicidade entre a privacidade e a intimidade, bem como a correlação entre a privacidade e a informação, para ao final se discutir as situações em que a cessão de informação é indispensável e a sua necessidade de proteção.

2

A tutela da privacidade e a informação

Sabe-se que o homem é um centro de referência de informações, que se não forem bem manuseadas podem representar perigo à privacidade do seu titular. Na sociedade da informação, marcada pela complexidade e velocidade das relações sociais e comerciais, estas informações são transmitidas de forma instantânea, ocorrendo em uma escala sem precedentes,

Como ser livre, o homem tem direito de conhecer e controlar as informações acerca de si. Na sugestão do Tribunal Constitucional Alemão, isso configura a liberdade informacional ou autodeterminação informativa.

Entende a liberdade informativa como uma condição indispensável ao livre desenvolvimento da personalidade e, consequentemente, situada no âmbito da vida privada. A autodeterminação informativa é a capacidade de o indivíduo controlar suas próprias informações, protegendo-se contra a coleta, o armazenamento, o uso e a revelação de seus dados pessoais.

É importante mencionar que neste trabalho, os termos "dados" e "informações" serão utilizados como sinônimos, não obstante alguns autores prefiram diferenciar as referidas expressões, como foi visto no capítulo anterior[1]. Justifica-se tal opção pelo fato de que os dois termos, na maioria das vezes se sobrepõem, representando um aspecto da realidade[2].

---

[1] Ver Danilo Doneda (2006, p. 152).

[2] A Directiva 95/46/CE, no seu art. 2° definiu dados pessoais como: "qualquer informação relativa a uma pessoa singular identificada ou identificável".

Nesse capítulo, pretende-se analisar a evolução conceitual do direito à privacidade, desde o seu conceito tradicional dado por Warren e Brandeis até a noção mais contemporânea, representada pela autodeterminação informativa.

Em seguida, demonstrar-se-á a cumplicidade entre privacidade e intimidade. Não obstante as várias tentativas doutrinárias para diferenciar ambas as expressões, verificar-se-á que muitos autores as utilizam como termos sinônimos, demonstrando assim, verdadeira confusão conceitual nesta matéria.

Após, analisar-se-á a relação entre a privacidade e a informação, já que o aspecto que está sendo investigado neste trabalho é aquele referente à privacidade informacional, identificando os possíveis riscos nesta matéria. Ao final do capítulo, pretende-se analisar situações em que a transmissão de informações é indispensável, como nos casos de garantia da segurança nacional, muito embora a transmissão de informações só possa ocorrer, via de regra, com a autorização do seu titular.

2.1 A evolução conceitual do direito à privacidade

Não tem sido tarefa fácil a delimitação conceitual do bem *privacidade*. Desde as primeiras manifestações teóricas, juristas e filósofos tentam firmar o conteúdo e as fronteiras do direito à privacidade. Não houve, porém, um conceito capaz de atravessar os tempos, a influência cultural na delimitação dos interesses tuteláveis pelo direito à privacidade.

Por meio do artigo intitulado *Right to privacy,* os juristas norte-americanos Warren e Brandeis (1890) delinearam os contornos de um conceito tradicional de privacidade. A ideia de escrever esse trabalho surgiu, em primeiro lugar, por vontade de Warren, que após ter se casado com a filha do Senador Thomas F. Bayard, tinha sua intimidade e privacidade constantemente devassadas. Como fazia muitas recepções em sua casa, sofria a pressão da imprensa e dos jornalistas que queriam fazer os

registros. Incomodado com tal frequente assédio, convidou a Brandeis, um colega de universidade, para discutir o tema no artigo que se tornou pioneiro e fundamental para a análise da matéria. Importa lembrar que Warren era um conservador tradicional, preocupado com os privilégios da alta burguesia, encarando com ressentimento o assédio da imprensa à procura de escândalos políticos. O isolamento passou a ser um privilégio desta classe ou de alguns que por opção ou necessidade viviam longe das grandes cidades, como por exemplo, os monges.

Todavia, o incômodo apontado por Warren não teria sido o único foco da discussão. Também analisaram o caso *Manola vs. Myers*, um episódio ocorrido entre uma atriz famosa e o *The New York Times,* que relatou ao público os detalhes de sua vida pessoal[3].

No final do ensaio, Warren e Brandeis reafirmaram as fronteiras do *Right to privacy,* considerando que:

> a) o direito à privacidade não impede qualquer publicação de matéria que seja de interesse público; b) o direito de estar só não proíbe a comunicação de qualquer tema particular, quando é feito sob circunstâncias que não causam danos a outrem; c) a lei não ofereceria qualquer meio contra a invasão da intimidade pela divulgação oral, na ausência de dano especial; d) cessa o direito à vida privada, com a publicação de fatos pelo interessado ou com seu consentimento; e) a verdade da alegação não serve como defesa (WARREN; BRANDEIS, 1890, p. 205)

Percebe-se que o *Right to privacy,* idealizado pelos juristas norte-americanos, tem como foco principal a ação da imprensa, na divulgação de escritos, fotos, imagens, que digam respeito tão

[3] Em 1890, Marian Manola, em uma cena da peça de teatro *Castles in the air*, na qual aparecia com roupas íntimas, viu-se surpreendida sendo fotografada por Myers do famoso jornal americano *The New York Times*. Quando a atriz percebeu o que estava acontecendo, se cobriu com um cobertor e fugiu do palco no meio do espetáculo, resultando tal fato no processo *Manola vs. Myers* ajuizado junto à Suprema Corte de Nova York. O referido caso foi citado por Warren e Brandeis (1890) no *The Right to Privacy* no mesmo ano, na Harvard Law Review, considerando o direito à privacidade como *right to bet let alone*, concepção posteriormente adotada expressamente pela Suprema Corte americana (GLANCY, 1990, on- line).

somente à vida privada das pessoas e, que não tenham qualquer relação com o interesse público. Tal divulgação só seria admitida com o consentimento do interessado.

Sobre os argumentos utilizados pelas doutrinas jurídicas que tratam da privacidade no direito norte-americano, Amitai Etzioni (2012, p. 294) identifica três fases de desenvolvimento:

> a fase anterior a 1890 (utilizando-se de princípios do direito de propriedade para proteger a privacidade); a fase que vai de 1890 a 1965 (considerada como a fase em que se desenvolveu um direito à privacidade vinculado à ideia de isolamento) e; a última fase, posterior a 1965 (período que demarca a ampliação da noção de direito à privacidade).

Na primeira fase, a sociedade norte-americana, a exemplo das demais, tinha um conceito impreciso de privacidade, utilizando-se do direito à propriedade, que naquela época já era consagrado como um direito natural e um bem absoluto. Por esta razão, nesta fase havia uma correlação entre o direito à privacidade e à propriedade.

Etizioni (2012, p. 295) utiliza o ensaio de Warren e Brandeis como o marco a partir do qual a privacidade recebe atenção autônoma, inaugurando a segunda fase. Warren e Brandeis propuseram que o postulado original do direito à privacidade é conceitualmente diferente de outras liberdades, como o direito à propriedade, comum à época.

A privacidade, nesta perspectiva de isolamento, identifica características marcantes do pensamento jurídico próprio do paradigma moderno, enraizadas no jusnaturalismo e positivadas nos Códigos Civis com a ascensão da burguesia ao poder, como por exemplo, o individualismo, o viés patrimonialista e o perfil voluntarista. (KONDER, 2013, p. 357).

Nesse contexto, Rodotá (2008, p. 26) explica que a ideia de privacidade como isolamento naquela época era privilégio de poucos eleitos ou daqueles que, por necessidade ou opção viviam

distantes da comunidade, como os monges e pastores, sendo posteriormente estendida esta possibilidade a todos os que detinham os meios materiais necessários que lhes permitissem tal isolamento. Este foi um processo para o qual contribuíram vários fatores, que vão desde as novas técnicas de construção das habitações até a separação entre o lugar no qual se vive e o local de trabalho. Por esta razão, Rodotá (2008) entende que a privacidade configura-se como uma possibilidade da classe burguesa, que consegue realizá-la graças às transformações socioeconômicas relacionadas à revolução industrial.

A terceira fase citada por Etizion se inicia após 1965. Foi caracterizada por uma série de casos julgados em matéria de reprodução humana. Como exemplo cita o caso *Roe v. Wade,* em 1973, no qual o Tribunal ampliou ainda mais o direito à privacidade, eliminando proibições ao aborto, ainda que fixando alguns critérios a partir dos quais os Estados poderiam determinar a sua proibição (ETIZIONI, 2012, p. 301-302).

Nesse sentido, dependendo da opção doutrinária escolhida, podem-se encontrar conceitos abrangentes ou restritivos, como por exemplo, quando se analisa a privacidade como liberdade de pensamento, direito ao próprio corpo, recato, controle sobre informações pessoais, autodeterminação informativa, dentre outros.

O conceito de privacidade se mostra como muito vago e indeterminado, o que faz parecer que ninguém tem uma ideia muito clara do seu significado. Note-se que tal constatação não se dá apenas no âmbito nacional, como um problema isolado, mas também na doutrina estrangeira. Nesse contexto, observa-se que a maioria dos problemas que se referem ao conceito de privacidade tem relação com um esclarecimento conceitual insuficiente (PINTO, 1993, p. 506).

Na verdade, tem-se de um lado os conceitos unitários de privacidade, abarcando por sua vez, o direito a ser deixado só; o resguardo quanto às interferências alheias; o controle sobre

informações pessoais e; de outro, a noção de um direito geral à privacidade, que se aplica em todas as situações.

A privacidade como "direito a ser deixado só", formulado por Warren e Brandeis (1890), em seu célebre trabalho, que influenciou a doutrina e jurisprudência não só norte americana como também de outros países, revela-se com um significado muito vago. Esta perspectiva deve ser entendida como uma espécie de isolamento social, marcado por um individualismo exacerbado.

Nos EUA, apesar de diversos casos levados aos tribunais, envolvendo direta ou indiretamente, aspectos do *Right of privacy,* não houve um desenvolvimento retilíneo desse direito, conforme analisa Sampaio (1998, p. 63-64). O referido autor recorda que, os julgados proferidos entre 1890 e 1950 mostram que muito embora não tenha havido um reconhecimento imediato desde direito, as ideias dos seus principais expoentes, já podiam ser percebidas nas primeiras sentenças prolatadas desde então.

Já em 1891, se reconheceu, em *Mackenzie v. Soden Mineral Springs Co.,* que o uso desautorizado do nome e da assinatura de um médico famoso era uma violação ao "razoável direito à privacidade". Em outro caso, *Marks v. Joffa,* o mesmo tribunal de Nova Iorque, julgou ilegítima a publicação da fotografia de um autor, formando parte de um concurso de popularidade ao qual se opunha. Nestes casos a privacidade foi definida como r*ight to be let alone* (SAMPAIO, 1998, p. 64).

Nesse sentido, malgrado o acolhimento da jurisprudência norte-americana ao *right to privacy,* percebia-se certa insegurança entre os juristas no que se refere a sua aceitação generalizada, isto porque somente em 1939, a privacidade foi reconhecida como direito pelo *Restatement of Torts.*

Com relação ao resguardo contra interferências alheias, percebe-se que esta noção muito se aproxima da ideia de isolamento. No entanto, não se trata de conceitos equivalentes, mas tão somente do direito que o indivíduo tem de manter certos assuntos da sua vida

privada para si, bem como o direito de decidir em que medida eles serão levados ao público (LEONARDI, 2012, p. 56).

É muito problemático se conceituar privacidade como o direito à proteção contra as interferências alheias. Afinal, nem todas essas interferências caracterizarão violação à privacidade. Somente produzirá lesão à privacidade, aquela intervenção, cujos limites não estão bem delineados e que toca em informações mais sensíveis ao titular. Assim como é vaga a restrição conceitual da privacidade ao "direito de estar só"; também o será, aquela conceituação que limita a privacidade à proteção contra as interferências alheias.

Outro conceito unitário de privacidade, todavia, mais contemporâneo, é o que a relaciona ao controle das informações pessoais. Privacidade seria o direito que tem o indivíduo de controlar a circulação das informações a seu respeito. Nesse contexto, ele escolherá o conjunto de informações que pretenda manter sobre o seu exclusivo controle, protegendo-as da interferência ilegítima de terceiros. Nos dias atuais, pode-se afirmar que a noção ora analisada é uma das mais relevantes para o direito à privacidade. Distingue-se da noção anterior de privacidade, pois aquela se refere à ausência de conhecimento alheio sobre fatos da vida privada do indivíduo e, esta vincula-se à ideia de controle exercido sobre as informações pessoais que lhe digam respeito.

Observa-se, dessa forma, que o direito à privacidade mostra-se em algumas situações como um direito à liberdade. Todavia, esta liberdade é uma expressão que também revela alguma dificuldade na sua conceituação, sendo um dos temas mais desafiadores no campo da ciência social. Por esta razão, Sampaio (1998, p. 264) analisa a liberdade pelo seu duplo sentido filosófico: no sentido de não intromissão e de autonomia ou direito de escolha. A não intromissão delimita um espaço individual de exclusão e permite a concretização de um sentido afirmativo da personalidade.

O sentido de liberdade que mais se coaduna com a noção de privacidade que ora se analisa é a autodeterminação informativa, cujo fundamento está na liberdade como autonomia (direito de escolha). Importa na prerrogativa que tem o indivíduo de escolher quais informações pretende transmitir ou não para terceiros.

Assim, sem uma tutela efetiva dos dados que digam respeito à determinada pessoa, a sua personalidade está cada vez mais ameaçada de ser discriminada por suas opiniões, crenças religiosas, filosóficas e políticas. Dessa forma, a privacidade se apresenta como um elemento fundamental da sociedade de igualdade, como ensina Rodotá (2008, p. 233).

Consequentemente, se o cidadão não tiver uma tutela efetiva em relação às suas informações referentes a convicções políticas, a inserção em partidos, sindicatos ou associações, sofrerá ameaça de exclusão dos processos democráticos. Nesse sentido, a privacidade passa a ser uma condição essencial para inclusão na sociedade de participação. Sem uma forte tutela dos dados pessoais, a própria liberdade pessoal está em perigo (RODOTÀ, 2008, p. 233).

No entanto, sabe-se que o controle sobre tais informações pessoais não pode ser total e absoluto, isto porque existem situações nas quais é imprescindível a sua cessão. Saber quais informações sobre determinado indivíduo podem ser objeto de controle enfrenta dificuldades, sendo mais uma razão para a necessidade de se regulamentar esta matéria no Brasil, com a devida fixação de limites a tal controle.

Muito comum ao se tratar do conceito de privacidade é se recorrer às noções de "vida pública" e "vida privada". Se compreendidas como expressões antônimas, tem-se a pretensão de considerar como pública, a vida social do indivíduo, e como privada, o conjunto de fatos relacionados à sua vida familiar e pessoal, como aqueles de interesse mais restrito.

Observa-se que essa noção de vida pública, porém, não se refere ao conceito usual de política, isto porque pessoas estranhas à atividade política podem também ter uma vida pública, a exemplo

dos artistas, em geral. Há determinadas profissões que são exercidas sobre um palco ou à frente das câmaras de televisão, de sorte que a publicidade é inerente à atividade destas pessoas.

Fernandes (1996, p. 250) considera simplista e problemática uma distinção nesses termos, na medida em que pode permitir alguns equívocos. Invocando a doutrina alemã das esferas de Hubman, o autor lembra que a atividade laboral, ainda que realizada no ambiente da vida privada, não recebe a mesma proteção daqueles aspectos mais restritos atinentes aos assuntos domésticos e familiares.

Nos dias de hoje, revela-se ainda mais complexa a identificação das esferas pública e privada. Nenhuma vida humana é possível sem um mundo que envolva a presença de outros seres humanos. Por esta razão, a pessoa humana deve ser analisada pela perspectiva de ser titular de duas vidas, a pública e a privada (ARENDT, 1995, p. 31-33).

Percebe-se como é difícil estabelecer onde termina a vida privada e começa a vida pública. Dessa forma, entende-se que não há um critério válido para uma separação estanque entre as duas expressões. Alguns autores sugerem que eventual distinção dependeria de fatores como o tempo, o lugar, a cultura e as condições econômicas de cada sociedade (FERNANDES, 1996, p. 251-252).

Com o passar dos anos, o debate acerca da privacidade foi se acalorando e mudando de foco, principalmente com o surgimento das novas tecnologias de informação e comunicação, mais notadamente com o advento do computador. Com essa revolução tecnológica, a tutela da privacidade passou ser um problema ainda mais premente e que inspira todos os cuidados por parte dos indivíduos.

A presente discussão não se refere apenas ao tema clássico da defesa da esfera privada contra as invasões externas, tendo havido uma mudança qualitativa. Os problemas da privacidade, nos dias atuais, se referem ao âmbito da informação,

representando um dos componentes fundamentais (RODOTÁ, 2008, p. 23-24).

Atualmente, pode-se afirmar que a privacidade é matéria de interesse global, pelo menos nos Estados constitucionais modernos. Inúmeros estatutos, leis e decisões judiciais podem ser apresentados com o fito de proteger esse direito. Nesse sentido, Etizioni (2012, p. 304) fala que os direitos da personalidade, em geral, e a privacidade, em especial, estão muito mais protegidos nos dias de hoje, nos Estados Unidos, do que estiveram nos idos de 1890.

Não obstante, ainda perseveram opiniões doutrinárias diversas acerca do seu conceito e do seu conteúdo. Por esta razão, é relevante o papel da jurisprudência na construção do conceito, dos limites e do conteúdo do que seja privacidade. Julgado interessante do Superior Tribunal de Justiça, em sede de Recurso Ordinário[4], tratou sobre a privacidade nas comunicações telefônicas. No caso, um marido suspeitando a traição da esposa, interceptou sua conversa telefônica com o respectivo amante e, depois, utilizou a gravação em processo criminal que acusava a mulher de ministrar tóxicos para as filhas menores.

Solove[5] lamenta que a privacidade seja um conceito em desordem, cuja abrangência engloba, dentre outras coisas, a liberdade de pensamento, o controle sobre o próprio corpo, a solidão em sua casa e o controle sobre informações pessoais. Ainda que não tenha proposto uma teoria autônoma para resolver os problemas conceituais acerca da privacidade, ofereceu uma estrutura específica para análise dos processos envolvendo a matéria.

---

[4] O Superior Tribunal de Justiça entendeu que o marido não poderia ter gravado a conversa ao arrepio do seu cônjuge, ainda que impulsionado por motivo relevante, acabando por violar a intimidade de sua esposa, direito garantido constitucionalmente (art. 5°, X). (RMS n° 5352/GO. Rel. Min. Adhemar Maciel. Julgado em: 27 de maio de 1996. Diário de Justiça em 25 de novembro de 1996. Disponível emhttp://www.stj.gov.br/SCON/jurisprudencia. Acesso em: 30 de jun. 2014.

[5] Daniel J. Solove is the John Marshall Harlan Research Professor of Law at the George Washington University Law School. He is a Senior Policy Advisor at Hogan Lovells. He is also the founder of TeachPrivacy, a company that provides privacy and data security training programs to businesses, schools, healthcare institutions, and other organizations.

Considerando que os tribunais, em geral, mantêm uma visão unitária sobre privacidade quando avaliam um caso concreto, Solove (2006, p. 480-481) desenvolve uma taxinomia sobre os diferentes tipos de atividades que podem afetar o direito à privacidade, de modo a favorecer a prestação da tutela jurisdicional correspondente. Pretendia, com isso, conferir maior clareza conceitual à temática.

Prosser (1960) identificou quatro tipos de atividades nocivas à privacidade: a intromissão em assuntos particulares do indivíduo; a divulgação pública de fatos particulares embaraçosos ao indivíduo; a publicidade que coloca o indivíduo em uma situação difícil aos olhos do público e a tirada de vantagens do nome do indivíduo. Observa-se, porém, que com essa divisão, Prosser (1960) apenas sintetizou os casos que emergiram após o artigo de Warren e Brandeis. Até porque, naquela época não poderia suscitar os problemas específicos da era da informação.

Dessa forma, Solove (2006, p. 482) busca uma mudança de foco, com o objetivo de se afastar da vagueza que o termo apresenta, mostrando outras atividades específicas como problemas que podem afetar a privacidade. Entende a privacidade como um conceito genérico, do qual decorem várias especialidades (SOLOVE, 2006, p. 485). Na taxinomia que propõe, procura identificar as conexões entre os diferentes danos e problemas, bem como entender onde eles divergem (p. 486). Assim, conclui que há quatro grupos de atividades prejudiciais à privacidade: "i) a coleta de informação; ii) o processamento de informações; iii) a disseminação das informações e, iiii) a invasão. Cada grupo sendo constituído por vários subgrupos" (SOLOVE, 2006, p.488).

A coleta de informações pode ser realizada tanto por pessoa física quanto por entidades públicas ou privadas. Nem sempre a coleta de informações repercutirá negativamente para o seu titular. No entanto, é possível que algumas delas venham a causar prejuízos, se processadas indevidamente. Como exemplo, citam-se aquelas informações pertinentes à orientação sexual, à convicção

política, religiosa ou filosófica etc. No processamento desses dados, quando se faz o armazenamento e a manipulação, eles podem sofrer distorções e resvalar em ofensa à privacidade do titular.

Em seguida, passa-se a fase de disseminação das informações, descrita por Solove (2006, p. 488-489), como aquela na qual os detentores dos dados fazem a sua transferência para terceiros. Da coleta para o processamento é que as informações se distanciam do controle de seus titulares, assim como aumentam os riscos de danos à privacidade, haja vista a possibilidade de distorção da informação disseminada.

Por último, tem-se a fase da invasão, que nem sempre diz respeito a informações, pois pode resultar de uma intrusão ou de uma interferência no processo de decisão. A primeira envolve casos de invasões na vida das pessoas, perturbando-as em atividades diárias e alterando a sua rotina. Já os casos de interferência de decisão estão ligados às informações ou decisões que a pessoa não deseja que sejam divulgadas, a exemplo das decisões pertinentes ao planejamento familiar, à orientação sexual, etc.

A taxinomia sobre privacidade desenvolvida por Solove (2006) possui extrema importância na discussão do objeto desta pesquisa. Nela se cotejam, em grande medida, as informações pessoais, que após serem manipuladas ou tratadas, para posterior disseminação, podem ser devastadoras à privacidade de seus titulares. E o que se revela mais perigoso nesse assunto, é exatamente a ausência de conhecimento dos riscos de lesão à privacidade, aos quais estão submetidas às pessoas que disponibilizam os seus dados.

Nesse sentido, Sampaio (1998, p. 370) diz que há quem defenda que o verdadeiro ataque à privacidade se opera com a divulgação de alguns dados, fatos ou situações de caráter reservado e não com o simples conhecimento. Assim, somente a divulgação das informações de caráter mais reservado poderia ensejar a violação à privacidade. Também não seria necessária uma prévia investigação ilegítima para expor a pessoa quanto às informações

desse jaez. Afinal, um amigo ou um irmão poderá divulgar fatos da intimidade de outro, conhecidos em decorrência do ambiente familiar, cometendo assim, violação à privacidade daquele.

Comumente, pessoas que contratam com instituições financeiras, operadoras de telefonia, serviços de internet e outros tipos de contratos, são condicionadas ao fornecimento de informações pessoais, sob pena de não concluírem a contratação. Até então, não há qualquer sorte de problemas, considerando que estas informações são indispensáveis para celebração destes contratos. São informações gerais sobre o sujeito que não tocam àqueles chamados dados sensíveis[6].

A par da taxonomia de Solove, observa-se uma profusão de conceitos que por se apresentarem ora muito abrangentes, ora muito restritivos ou vagos não logram a adesão unânime da doutrina (LEONARDI, 2012, p. 79). Em razão da polimorfia do seu objeto, a privacidade demanda a sua tutela por meio de um direito geral à privacidade, capaz de abarcar todas as suas manifestações.

O direito geral à vida privada, segundo Sampaio demanda uma compreensão muito mais ampla, fundamentada na ideia de autonomia privada e na noção de livre desenvolvimento da personalidade e que alcança, sem embargo, certos desdobramentos (SAMPAIO, 1998, p.274). Tais desdobramentos são produtos de uma determinada realidade social, econômica e política, perceptível pelo pensamento jurídico contemporâneo.

Embora o seu conteúdo possa ser determinável em certo lugar e tempo, estará sempre aberto a novas interpretações, acréscimos e reduções, acompanhando, assim, a própria evolução da sociedade. Pode-se afirmar que o conteúdo do direito à privacidade é dinâmico, assim como dinâmica é a própria sociedade.

---

[6] Dados sensíveis são aqueles que se referem às convicções religiosas, filosóficas, políticas, orientação sexual e outros. Sem uma forte tutela destes dados, a pessoa está cada vez mais ameaçada de ser discriminada. Nesse caso, a privacidade se apresenta como elemento fundamental da sociedade de igualdade (RODOTÁ, 2008, p. 233).

A ideia de um direito geral é mais compatível à conjuntura social e jurídica atual do que qualquer compreensão reducionista sobre privacidade. A tutela da pessoa na sociedade informacional requer um direito capaz de oferecer suporte protetivo naquelas circunstâncias que escapam os limites dos direitos especiais de personalidade e, por que não dizer, de privacidade.

Por outro lado, não há qualquer problema em se analisar a privacidade de acordo com as situações concretas apresentadas, isto porque, de uma forma ou de outra, o que se pretende é a tutela efetiva da privacidade, como direito integrante da personalidade humana. Nesse sentido, importa lembrar que a privacidade pode ser analisada como direito de defesa e como direito à prestação, de acordo com a classificação sugerida pelo critério funcional de Jelinek[7]. Como direito de defesa, desponta o seu caráter negativo, que significa o direito que tem o titular de exigir do Estado e dos particulares uma abstenção de intervenção da sua esfera jurídica. Trata-se da prerrogativa de impor respeito à sua intimidade e à sua vida privada (MENDES; BRANCO, 2014, p. 157).

Pode-se encontrar este caráter negativo no art. 5º, X da CF/88 – "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". (BRASIL, 1988)

Na condição de direito de defesa, o direito à privacidade, confere ao seu titular os direitos subjetivos de pretensão, de abstenção e pretensão de consideração (VIEIRA, 2007, p. 97). No primeiro, requer-se a não intromissão por parte do Poder Público e demais particulares na sua intimidade e vida privada. De acordo com o segundo, exige-se do judiciário e do legislativo a

[7] A teoria dos quatro *status* foi desenvolvida por George Jellineck, jurista e filósofo que viveu a maior parte da sua vida na segunda metade do século XIX. Segundo a referida teoria são quatro os *status d*o indivíduo na sua relação com o Estado: No s*tatus* passivo, o indivíduo encontra-se em posição de sujeição em relação ao poder público; no *status* ativo, o individuo tem o poder de interferir na vontade do Estado; no *status* negativo, o Estado não poderá intervir nas ações do indivíduo. Podendo autodeterminar-se sem ingerência estatal e, no *status* positivo, o indivíduo poderá exigir do Estado ações positivas em seu favor.

consideração do direito à privacidade em hipótese de colisão com outros direitos fundamentais.

O direito de defesa também protege bens jurídicos contra ações do Estado, como por exemplo, em face do direito à vida, o Estado não poderá assumir comportamentos que violem a existência do ser humano, assim como, em face do direito à privacidade, o Estado não pode divulgar dados pessoais dos seus cidadãos. Assim, o direito de defesa ganha forma de direito a não abstenção dos bens protegidos (MENDES; BRANCO, 2014, p. 158).

Atualmente, discute-se que a efetivação do direito à privacidade requer não só uma abstenção por parte do Estado e dos demais particulares, mas também uma atitude positiva, com o fim de garantir a não intromissão de terceiros na intimidade e na vida privada das pessoas. Trata-se de expressão do *status* positivo de Jelinek e dos direitos a prestação.

Os direitos à uma prestação partem do pressuposto de que o Estado deve agir para libertar os indivíduos das necessidades, ou seja, buscam fornecer as condições materiais indispensáveis ao desfrute efetivo das liberdades asseguradas nos direitos de defesa. Exige-se um comportamento ativo do poder público em prol da sociedade. Gilmar Mendes (2014, p. 160) lembra que o direito à prestação pode referir-se quer a uma prestação material, quer a uma prestação jurídica.

Os direitos a prestações materiais são denominados de direitos à prestação em sentido estrito, resultando da concepção social de Estado, são os direitos sociais por excelência. Já os direitos à prestação jurídica, têm como objeto, não uma satisfação material, mas sim uma normatização do bem jurídico protegido como direito fundamental. Esta prestação pode se apresentar como norma jurídica ou normas de organização e de procedimento.

Em outro sentido, Castro (2005, p. 28), analisando o direito à autodeterminação informativa, destaca duas dimensões: uma subjetiva e outra objetiva. Na dimensão subjetiva, apresenta-se como o direito que garante ao titular posições jurídicas perante o

Estado, a fim de protegê-lo dos abusos decorrentes da utilização de sua informação pessoal. Já na sua dimensão objetiva, a autodeterminação informativa impõe a adoção de medidas de proteção pelo Estado.

Nesse contexto, a privacidade, como autodeterminação informativa, tanto pode se configurar como direito de feição negativa, como também por uma dimensão positiva, consubstanciando-se no poder de controlar informações pessoais que estejam em poder do Estado ou de outras pessoas privadas.

O Tribunal Constitucional Alemão, ao julgar o caso do Censo de 1983, em virtude do qual se exigia dos cidadãos alemães, o preenchimento de um questionário que serviria tanto para fins estatísticos como também para outros fins, conferiu s*tatus* constitucional à proteção de dados pessoais, sendo garantido a todos os cidadãos alemães o direito de recusar informações de caráter pessoal. Com isso, sustentou o direito à autodeterminação informativa como um dos aspectos da privacidade. Em última instância, afirmou-se a decisão no valor da dignidade da pessoa humana que deve ser respeitado e protegido como o centro do sistema constitucional e pressuposto de uma sociedade livre (RODOTÁ, 2008, p. 234).

Ainda que o fundamento da privacidade haja sido encarado de modo distinto pelos europeus e americanos, na medida em que os primeiros correlacionavam-na à ideia de dignidade da pessoa e os últimos aos ditames da liberdade, os dias de hoje já não admitem essa bipolaridade. Tanto é que a Carta dos Direitos Fundamentais da União Europeia já informa a liberdade como fundamento da privacidade. Sistematicamente, o direito à proteção de dados foi posicionado na parte dedicada à liberdade (RODOTÁ, 2008, p. 236). De outro lado, o modelo norte-americano envolve elementos que reconduzem a privacidade ao conceito de dignidade, como por exemplo, quando tutela as escolhas existenciais contra o poder público. Pretende-se evitar que as escolhas da vida sejam condicionadas por pressões públicas ou privadas.

Nesse contexto, a reconstrução das relações entre privacidade/dignidade e privacidade/liberdade alcança fundamental importância para o estágio atual da sociedade, caracterizada pelo alargamento progressivo das formas de controle social. Vive-se a chamada sociedade de vigilância, as mais novas tecnologias da informação e comunicação permitem extrair o indivíduo da massa, criando-se perfis individuais, familiares ou de grupo, que comprovam a mais absoluta falta de controle no que se refere à observação e à vigilância.

A vigilância passou a ser cotidiana, deixou de ser excepcional. Não só as pessoas que apresentam "perigo" para sociedade são vigiadas, mas também toda a massa de indivíduos. Rodotá (2008, p. 238) observa que alguns estudiosos norte-americanos fundamentam esta nova feição da vigilância na "democratização", excluindo todas as formas de seleção dos investigados. Se todos são controlados e fechados, todos são tratados de forma igual.

Não obstante, essa noção de vigilância acaba por violar a dignidade e a liberdade das pessoas, considerando que todos os indivíduos acabam sendo suspeitos. Destaca-se, por oportuno, que a vigilância não diz respeito somente à imagem das pessoas, mas também aos seus dados, suas informações pessoais, o que importa para o presente trabalho.

Ao analisar a questão dos excessos na sociedade de vigilância e a possibilidade de violação da dignidade humana, Rodotá (2008, p. 239-240) observa que está ocorrendo a erosão das prerrogativas da pessoa. Assiste-se a transformação do seu próprio corpo, quando, por exemplo, o Reino Unido noticiou que os criminosos ingleses mais perigosos seriam etiquetados e acompanhados, por intermédio da inserção de *microchip,* Nota-se que tal situação convive de forma conflitante não só com a dignidade, recordada há pouco, mas também com a própria noção de pessoa evidenciada na Carta dos Direitos Fundamentais da União Europeia, na qual o direito à proteção de dados constitui elemento essencial.

Atualmente, a proteção à pessoa se apresenta como uma tutela global, abrangendo não só o seu corpo físico, mas também o seu corpo eletrônico, fazendo parte integrante da sua personalidade. O controle sobre este corpo eletrônico, ou seja, dados/informações deve ser considerado como prerrogativa de toda pessoa humana.

Todavia, tal direito ao controle exige por parte dos Estados uma regulamentação específica a fim de se imporem limites às atividades de coleta, armazenamento, manipulação e divulgação de informações pessoais, bem como de criar organismos fiscalizadores desta atividade.

2.2 A cumplicidade entre privacidade e intimidade

É importante analisar a estreita relação entre privacidade e intimidade. Não há uniformidade no emprego desses termos pela doutrina e/ou pelo ordenamento jurídico dos diversos países. Nos EUA, por exemplo, prefere-se o termo *Right of pivacy;* na França, *de droit à la privauté,* além da expressão *droit a l'intimité;* na Itália, predomina o termo d*iritto alla riservatezza,* ainda que alguns autores preferiram a expressão *diritto allá vita privata.*

Já na Espanha pode-se encontrar expressões como *derecho a la intimidad e derecho a la vida privada.* Em Portugal, fala-se em direito à proteção da intimidade e direito à intimidade da vida privada. O fato é que, além das várias designações dadas ao direito à privacidade e à intimidade, tem-se ainda outra discussão, a de saber se ambas as expressões são sinônimas ou não.

No Brasil, fala-se em privacidade, vida privada, intimidade, segredo, sigilo e recato, empregando-se uma profusão de termos para se referir, na verdade, à privacidade. A Constituição Federal de 1988, art.5º, X preferiu declarar invioláveis a intimidade, a vida privada, a honra e a imagem, não utilizando a expressão privacidade. Mesmo assim, a doutrina brasileira parece ter optado pelo termo "privacidade". Silva (2001, p.200) é um dos que

preferem utilizar a expressão "direito à privacidade", por entender ser mais ampla e genérica para abarcar as diversas manifestações que o texto constitucional consagrou.

Não obstante a preferência, a privacidade é, como já foi referido, um conceito jurídico indeterminado, assim como o são a liberdade e a dignidade da pessoa humana. Embora essa característica seja positiva para albergar as diversas manifestações da personalidade, pode gerar ambiguidades perniciosas (GROSS, 1967, p. 34-35).

Leonardi (2012, p. 47) explica que a falta de clareza a respeito do que seja privacidade cria complicações na resolução de casos práticos. Em caso de interesses conflitantes, como na hipótese de conflito entre privacidade e liberdade de expressão, o sopesamento pode conduzir a tolerância quanto aos danos à privacidade[8].

Mesmo assim, como já se afirmou neste trabalho, optar-se-á pelo termo privacidade, como um direito geral, no entanto, pode-se identificar nesse contexto, o direito à intimidade. Dessa forma, como se correlacionam a intimidade e a privacidade? Seriam expressões sinônimas ou a intimidade é um aspecto da privacidade?

Recorrendo a lição de Alonso (2005, p. 17), que entende as duas expressões como distintas, a intimidade seria o âmbito interior da pessoa, o espaço mais profundo, mais recôndito, secreto ou escondido. Algo inacessível, invisível, que só ela conhece. Na intimidade, a pessoa constrói-se e descobre-se a si própria. Para esse autor, ainda que se fale em direito à intimidade, esta é anterior ao direito. Em virtude do seu caráter originário, o direito a

[8] Tome-se como exemplo o "caso Cicarelli", em que a modelo Daniela Cicarelli foi flagrada fazendo sexo em uma praia da Espanha. O ex-namorado da modelo, Tato Malzoni ingressou com ação de indenização por violação a sua intimidade, por conta de um vídeo que fora divulgado no site *Youtube*. No entanto, o Tribunal de Justiça de São Paulo decidiu que o Google, *site* controlador do *Youtube,* não deveria pagar nada, argumentando que não houve qualquer conduta ilícita na divulgação do vídeo, já que o casal assumiu o risco quando escolheu um local público para a prática do ato.

ela se refere, pois sem intimidade não haveria pessoa, nem sujeito de direito.

Já a privacidade, para Alonso (2005, p. 17-18), situa-se no âmbito jurídico, isto porque a pessoa já praticou atos humanos, visíveis, tangíveis. Assim, para o citado autor, a distinção entre intimidade e privacidade está relacionada aos atos humanos. Os atos humanos quando internos, pertencem à intimidade, enquanto os atos humanos externos situam-se na privacidade. Explica-se:

> Os atos humanos são preparados ou elaborados na intimidade e, uma vez elaborados, permanecem no interior ou aparecem externamente, segundo forem atos internos ou externos. A preparação do ato humano e aqueles atos humanos que permanecem dentro de nós, sendo apenas internos, pertencem à *intimidade*. Alguns atos externos, aqueles que a própria natureza reserva ou a pessoa quer reservar e pode reservar para si, por não prejudicarem terceiros, pertencem à privacidade (ALONSO, 2005, p. 17).

Ao analisar outro aspecto da privacidade, Sampaio (1998, p. 367) lembra que o direito civil brasileiro traz regras sobre o uso nocivo da propriedade, atribuindo-se ao proprietário e ao inquilino o direito de impedir o mau uso da propriedade vizinha capaz de prejudicar o sossego, a segurança e a saúde dos que ali habitam. Essa perspectiva, ainda que importante, não é suficiente para tratar da privacidade. Nos dias atuais, repita-se, ocorre a erosão dos conceitos tradicionais de privacidade, pois a tutela do recato, da vizinhança, da intimidade já não é suficiente (DOTTI, 1982, p. 335).

Atualmente, as agressões à privacidade podem afetar a própria qualidade de vida a que todas as pessoas têm direito de usufruir. Podem repercutir no seu direito de se auto afirmar, nas suas escolhas pessoais, profissionais e, inclusive, suscitar problemas de discriminação. A tecnologia permite a interceptação de conversas, a gravação e a multiplicação da voz, da imagem, das atitudes e das emoções, a identificação de códigos genéticos, o diagnóstico de doenças etc., que podem conduzir a existência

humana a uma experiência de plena transparência. Com essa arquitetura dos dados pessoais constroem-se os murais da indiscrição muito maiores que as barreiras da privacidade (DOTTI, 1982, p. 335).

Quanto à cumplicidade entre privacidade e intimidade, tem-se que a privacidade traduz uma faculdade inerente ao ser humano de obstar a intromissão de estranhos em sua intimidade e vida privada, bem como de controlar as suas próprias informações, com o objetivo de evitar que estes dados sejam divulgados sem autorização do seu titular.

Verifica-se que a intimidade é algo a mais encoberto que a vida privada. Traduz-se como aquele espaço impenetrável, intransponível, que diz respeito apenas à pessoa. A intimidade envolve aquelas informações que o titular não deseja compartilhar, porque consubstancia os seus segredos, suas particularidades e suas expectativas mais singulares (GUERRA, 2004, p. 55).

A intimidade está no núcleo essencial da pessoa (ALONSO, 2005, p. 16-20) e deve ser protegida contra quaisquer intromissões, configurando a sua esfera mais reservada. Já a vida privada, seria todo ato humano externo, social, lícito, que a pessoa deseja preservar de divulgação e de conhecimento de terceiros (ALONSO, 2005, p. 24-25). Na visão desse autor, a intimidade não é compartilhada com outras pessoas, pertence apenas ao indivíduo em seu isolamento. Ao passo que, na vida privada há a participação daquelas pessoas íntimas ao indivíduo e, que por isso, têm acesso às informações sobre a vida pessoal e familiar.

Pinto (2002, p. 23) se utiliza do termo “direito à reserva sobre a intimidade da vida privada”, expressão de preferência do direito português. Mas explica que não se deve fazer confusão entre esse direito e o direito à proteção a vida privada. O primeiro tem por objeto o controle de informações pessoais. O interesse que visa proteger é o controle do conhecimento, da divulgação ou simplesmente da circulação da informação. Exclui-se, deste âmbito,

interesses que têm a ver com a liberdade de condução da vida privada.

Percebe-se que o direito à reserva sobre a intimidade da vida privada se apresenta pela confluência entre o controle sobre a informação e a esfera da vida privada, aceitando-se a extensão da noção de direito à autodeterminação informativa para além do domínio do tratamento de dados pessoais, como aspecto do direito geral de personalidade (PINTO, 2002, p. 24).

Quando Sampaio (1998, p. 268-269) analisa a relação entre intimidade e vida privada, faz uso das informações etimológicas, da linguagem cotidiana e do direito comparado. Do ponto de vista etimológico, intimidade deriva do latim *intimus q*ue significa "íntimo", "recôndito", "interior", referindo-se à ideia de segredo e confiança. *Privatus* deu origem a *privacy, privée. Privato e privada,* que significa "privado", "particular", "próprio" e "pessoal".

As expressões "intimidade" e "vida privada" no uso vulgar ou do cotidiano, têm um conteúdo mais próximo, senão equivalente, embora seja mais comum o uso do termo intimidade e de suas variantes, quando se trata, por exemplo, de assunto íntimo, reservado, exclusivo (SAMPAIO, 1998, p. 269).

Percebe-se que tudo dependerá do contexto no qual a expressão está sendo aplicada.

Quando se diz "ter intimidade", impõe-se um terceiro como titular desse espaço de reserva, implica-se uma qualidade que se tem perante o outro (SAMPAIO, 1998). Ser próximo a determinada pessoa, ter liberdade para expressar certos sentimentos e emitir opiniões. Assim como, quando se diz "invadir a intimidade", importa a intrusão no recôndito do sujeito, ou seja, se imiscuir em seus segredos e assuntos mais pessoais.

De outra forma, as locuções "vida privada" e "ter vida privada" não conduzem ao mesmo sentido de "ter intimidade". A vida privada é um atributo do sujeito da oração, diferentemente de "ter intimidade". Vida privada significa ter vida própria, autônoma (SAMPAIO, 1998, p. 269).

Observa-se, portanto, uma interminável confusão conceitual quando se trata de intimidade e privacidade. Alguns se referem a ambos os termos como sinônimos, enquanto outros fazem distinção, por compreenderem a intimidade como um aspecto mais íntimo e mais reservado que a vida privada.

Nesse sentido, é oportuno lembrar a doutrina alemã, notadamente a teoria das esferas ou dos círculos concêntricos, idealizada por Hubmann, para demonstrar a cumplicidade entre os termos privacidade e intimidade (COSTA JR, 2007). Na sua idealização, esses interesses estão resguardados sob uma estrutura semelhante a três círculos concêntricos.

O primeiro círculo e, de maior amplitude, representa a esfera da vida privada ou particular, composta por aspectos da vida pessoal que estão ao alcance da coletividade, em geral. Como estão sob exposição, esses aspectos estão excluídos do "campo dos chamados delitos de indiscrição" (COSTA JR. 2007, p.29). O segundo círculo, mais interior, refere-se à intimidade ou à confidência, cujo compartilhamento é restrito e depende da confiança e da intimidade. Por fim, o último círculo abrange o sigilo ou segredo, composto das manifestações guardadas em segredo pela pessoa, a salvo do conhecimento de todos os demais, inclusive, daqueles com os quais tem íntima relação de confiança. Verifica-se que esta classificação não se mostra tão diferente das anteriores, até porque, a divisão elaborada por Hubman foi tomada por muitos autores como base para compreender-se a distinção entre privacidade e intimidade.

Assim, percebe-se que a vida privada é a esfera de maior amplitude e envolve as manifestações da pessoa nos espaços em que transita e nas relações que mantém com todos os demais. Trata da vida particular da pessoa em sociedade.

A intimidade é a prerrogativa do indivíduo de excluir do conhecimento de terceiros as informações mais sensíveis, como por exemplo, orientação sexual, religiosa e política. Mesmo assim, o sujeito pode eleger as pessoas com as quais deseja compartilhar

essas informações. No âmago da privacidade estaria a esfera do segredo, que envolve as informações mais secretas que o indivíduo não deseja compartilhar com ninguém.

Ainda que Costa Jr. (2007) não suscite os casos de lesão à privacidade naquela esfera mais ampla, haverá sim, essa violação, sempre que houver malferimento à autodeterminação informacional, à divulgação distorcida ou desautorizada de dados. A violação da esfera da intimidade se faz preponderantemente por meio da divulgação desautorizada das informações. Já na esfera do segredo, a violação se daria por meio da intrusão violenta.

Destaca-se que a referida teoria dos círculos concêntricos, apesar de desenvolver uma tese para diferenciar a intimidade da vida privada, não deve ser analisada de forma rígida e engessada, isto porque a quantidade de círculos e a sua amplitude dependerão da categoria social a que o titular pertence, podendo ser flexibilizada.

A distinção entre privacidade e intimidade revela-se importante quando se avalia a responsabilidade civil por danos morais e/ou materiais nos casos de transmissão de informações pessoais não autorizadas, isto porque quanto mais íntima for a informação, tanto mais severa deverá ser a sanção, aumentando-se assim, o valor da indenização. No entanto, deve-se atentar para o fato de que mesmo as informações, aparentemente sem poder ofensivo, podem causar graves danos à privacidade, principalmente quando cotejadas com outros dados[9].

Importa destacar, por oportuno, que a privacidade e a intimidade, como direitos fundamentais não ostentam caráter absoluto, tendo em vista a multiplicidade de situações que podem levar ao conflito, fazendo com que o intérprete se utilize do método da ponderação, como foi explicado anteriormente.

---

[9] Trata-se da Teoria do Mosaico idealizada por Fulgêncio Madrid Conessa, que critica a teoria das esferas de Hubmam. Pela Teoria do Mosaico, o fato da informação pertencer a uma das esferas citadas por Hubmam é irrelevante, isto porque existem dados, que a princípio, podem ser inofensivos, até mesmo aqueles que pertencem à esfera da vida privada, que é a mais ampla das três. As informações pessoais devem ser protegidas, independente da esfera a que pertençam. (BESSA, 2003, 91)

Por conta da possibilidade de conflito entre direitos fundamentais, foi desenvolvida a teoria dos limites desses direitos, tendo como premissas básicas: que os direitos fundamentais não podem ser relegados a um plano secundário; e que a sociedade, em razão de sua complexidade e interesses multidirecionais, exige a solução de possíveis conflitos entre direitos fundamentais (SAMPAIO, 1998, p. 380).

Nesse sentido, percebe-se que a solução para os referidos casos não se mostra tão simples assim, a começar pela multiplicidade de tratamento que as Constituições de todas as nações dispensam ao tema. A limitação desses direitos pode se dá diretamente por prescrição constitucional expressa, ou indiretamente por intermédio de normas infraconstitucionais.

Assim, o direito à privacidade pode sofrer limitações por atuação legislativa direta, por intermédio de uma lei que incida diretamente sobre o âmbito de proteção do direito em análise, desde que haja autorização constitucional e indireta, considerando a conformação ou concretização de outro direito.

Sampaio (1998, p. 384), ao tratar da intervenção jurisdicional, destaca que a atuação dos órgãos jurisdicionais pode se dar em dois momentos: na autorização de medidas derrogatórias de aspectos do direito à intimidade e na solução de conflitos entre esse direito e outro bem ou interesse constitucionalmente protegido.

Considerando o objeto do presente estudo, não se tem a pretensão de analisar todos os conflitos que envolvem o direito à privacidade e à intimidade, mas tão somente aqueles que envolvem a autodeterminação informativa.

2.3 A relação entre privacidade e informação

Como já foi referido, ampliou-se o debate acerca da privacidade que passa a albergar, inclusive, o direito de controlar a coleta, manejo e divulgação das informações pessoais que se

refiram aos respectivos titulares. Conquanto a informação seja um direito muito aplicável ao *ciberespaço,* é necessária a sua regulação, mormente, quando toca em aspectos existenciais das pessoas. Tantas vezes, a circulação da informação nos espaços virtuais transcendem as fronteiras dos Estados, desafiando a capacidade de controle e intervenção (GONÇALVES, 2003, p. 7).

Sabe-se que os agrupamentos humanos sempre fizeram uso da comunicação. Na medida em que se desenvolviam, os meios de comunicação se aprimoravam. Atualmente são várias as formas de comunicação que transcenderam a era do rádio, da televisão e do telefone. Além dos meios de comunicação, por onde circulam as informações, houve um aprimoramento nas técnicas de coleta, codificação e transformação da informação, sobretudo, pelo uso do computador e da internet, ampliando-se as relações nesse *ciberespaço* (GONÇALVES, 2003, p. 8).

Os dias atuais são cenários de muitos atentados aos direitos à privacidade e intimidade, inclusive envolvendo menores, como por exemplo, a transmissão não autorizada de imagens e vídeos de nudez, sexo e pornografia. Imagens que se espalham rapidamente pelas redes sociais, causando danos irreparáveis às pessoas as cenas que ali são exibidas. Até os "comentários" ou "curtidas" apostos em redes sociais como, *Facebook,* podem acarretar consequências ou responsabilidades ao seu autor, dado a importância do papel da informação na vida das pessoas. Recentemente, o Tribunal Regional do Trabalho da 15ª Região, em sede de Recurso Ordinário, manteve uma decisão que tratava de demissão por justa causa de um trabalhador, que fez comentários ofensivos, através de *posts*[10].

[10] Na verdade, as ofensas foram escritas por um ex-funcionário, no entanto foram "curtidas" e comentadas pelo recorrente, com respostas cheias de onomatopeias que indicam gritos e risos. O recorrente utilizou-se de frases, do tipo: "Você é louco Cara... Mano vc é louco!". Pela forma como foi escrita, a Relatora Des. Patrícia Glugovskis Penna Martins, do TRT da 15ª região entendeu tratar-se de caso grave, já que as redes sociais têm um grande alcance, pois o recorrente confirmou que outros funcionários da empresa eram seus amigos no facebook. (Processo nº 0000656-55.2013.5.15.0002. Disponível em: www.migalhas.com.br. Acesso em: 26.06.2014.

Schneier (2001, p. 27), especialista em segurança de informações, explica que as ameaças no mundo digital espalham as ameaças no mundo físico. Exemplifica, que se os bancos físicos são roubados, os bancos digitais também o serão, isto porque a invasão da privacidade é a mesma. O agente do esbulho tanto pode ser o fotógrafo com uma lente telescópica ou *hacker* que invade as sessões de bate-papo particulares, ou a máquina particular de cada um. No Brasil, toma-se como exemplo, o "caso Carolina Dieckmann", que teve fotos pessoais, que estavam armazenadas no seu computador, divulgadas sem a sua autorização. Fato que contribuiu para a promulgação e sanção da Lei n. 12.737/2012, popularmente denominada de "Lei Carolina Dieckmann"[11].

Dessa forma, pode-se concluir que muitos dos crimes que ocorrem no *Ciberespaço,* se poderia esperar do mundo físico, como roubo, furto, extorsão, vandalismo, exploração e fraudes. A diferença é que nos crimes cometidos no ambiente virtual, há uma extrema dificuldade de se rastrear, capturar e condenar os autores do delito.

Na internet, podem-se identificar três características básicas, que qualquer uma delas isoladamente tem um efeito muito ruim, sendo que as três juntas congregam resultados ainda piores (SCHNEIER, 2001, p. 29). São elas: a automação, a ação à distância e a propaganda técnica. Por meio da automação, é possível a realização de tarefas tolas e repetitivas em um curto espaço de tempo, a exemplo da cunhagem de um milhão de moedas pelo falsário, enquanto ele dorme. A automação pode abrir grandes espaços para violação à privacidade.

A ação à distância denuncia que a internet não tem fronteiras ou limites naturais. É fácil estabelecer conexão entre um computador em São Paulo, a partir de outro instalado na Tunísia. Disso resulta que os agressores não precisam estar perto de suas vítimas, tornando a ameaça ainda mais difícil de ser rastreada e identificada.

[11]Lei 12.373/2012, denominada popularmente "Lei Carolina Dieckmann" – Dispõe sobre a tipificação criminal de delitos informáticos. Disponível em: http://www.planalto.gov.br. Acesso em 11 de jul. 2014

A última característica, a propagação da técnica, consiste na facilidade com que as técnicas bem-sucedidas podem se propagar pelo *ciberespaço*. Como exemplo tem-se a hipótese de divulgação de um sítio eletrônico da *web word wide,* voltado para a falsificação de dinheiro. Com um computador e um *scanner,* o falsário tem mais facilidade na criação de notas falsas.

Depreende-se pela análise acima, que a segurança no *ciberespaço* está correlacionada à ideia de controle. As pessoas que utilizam o ambiente virtual devem dispor de um controle sobre a sua utilização. Especialmente quando, alocam suas informações pessoais para uma determinada finalidade e estas acabam sendo repassadas a terceiros, sem a sua autorização, seja porque o primeiro destinatário as transmitiu, seja pelo fato de um *hacker* haver roubado essas informações.

Observa-se na Europa, a ampliação dos poderes de intervenção e controle para a tutela da privacidade. Conforme se verá no capítulo subsequente, atribui-se ao garante autoridade independente que opera com plena autonomia e independência de juízo e valoração, o poder de controlar o manejo e circulação das informações, nos termos do art. 28 da Diretiva 95/46/CE do Parlamento Europeu e Conselho da União Europeia, de 24 de outubro de 1995[12].

Na era da informação, às formas de tutela particular, soma-se a tutela pública da privacidade. Já não se trata da preservação do recato e do sossego, mas de uma proteção ampliada da personalidade na sociedade da informação, em face de inúmeras ameaças originárias da era digital, como por exemplo, as empresas que utilizam informações pessoais de seus clientes para outras finalidades não autorizadas. As formas tradicionais de tutela da privacidade são incrementadas para o enfrentamento dos problemas emergentes da sociedade atual.

[12] A Directiva 95 foi revogada em 2016 pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016.

Os processos digitais trazem problemas significativos que, na comparação de Solove (2004, p. 256), remetem à angústia narrada por *Franz Kafka,* no livro intitulado "O processo*",* no qual uma pessoa acorda com a inesperada presença de dois oficiais, declarando a sua prisão, sem qualquer razão aparente. O acusado sabe apenas que o Tribunal mantém um dossiê sobre sua vida, sem que ele próprio tivesse acesso ao mesmo.

Durante todo o romance, o protagonista tenta descobrir o motivo pelo qual o tribunal está interessado na sua vida ou a razão de sua prisão. No entanto, sua busca é vã. Com essa comparação, Solove (2004, p. 269) pretende ressaltar que as parcas leis existentes para proteger a privacidade das informações não são adequadas para enfrentar os chamados dossiês digitais. Seria necessária uma articulação mais apurada dos problemas que envolvem esta matéria, considerando o tempo presente com toda a sua complexidade que trouxe a era da informação.

A tutela da privacidade informacional não está confinada à atuação dos sujeitos particulares interessados. Na observação de Rodotá (2008, p. 199), envolve também uma responsabilidade pública específica. A demanda pelo controle público para a garantia da privacidade ressalta, por outro lado, a falta de credibilidade dos sistemas políticos centralizados, tecnocráticos e muitas vezes secretistas (GONÇALVES, 2003, p. 09). Os sistemas políticos que, segundo a citada autora, são incapazes de responder às expectativas e ansiedades de uma sociedade mais atenta aos riscos de origem tecnológica.

Entende-se que a tecnologia de informação deveria ser utilizada para fortalecer a democracia e não para favorecer a lesão de direitos da pessoa. Por esta razão, os governos deveriam disponibilizar *on-line* registros públicos, com informações não sigilosas, permitindo aos cidadãos a solicitação de informações, a expressão de opiniões e a consulta aos seus representantes, ao invés de concentrar seu uso nas questões de segurança. (CASTELLS, 2003, p. 128).

Entretanto, os recursos tecnológicos têm sido utilizados, preponderantemente, para a vigilância e o controle dos indivíduos. Consubstanciam-se muito mais como mecanismos de poder do Estado, do que como instrumento de fortalecimento da democracia representativa.

A vigilância na sociedade da informação está intrinsecamente relacionada ao exercício do poder disciplinar e os seus reflexos para os indivíduos e a coletividade. O exercício da disciplina tem como objetivo tornar o corpo mais obediente por meio de políticas de coerção e de manipulação do comportamento humano, como mecanismo para controlar de maneira minuciosa o corpo (FOUCAULT, 1988, p.127-129). Pela disciplina impõe-se a coerção com a utilização de pequenas astúcias e arranjos sutis, sem demonstrar a intensidade e gravidade do controle.

Como método de controle de comportamento dos indivíduos, a disciplina surgiu no âmbito das organizações religiosas e, posteriormente foi incorporada às instituições de ensino e fábricas. Absorvida pelo Estado, a disciplina é usada como um recurso apto a controlar o comportamento do cidadão, vigiando-lhe o passado e especulando o seu futuro.

Nessa perspectiva, é igualmente importante citar a obra *Panopticon,* de Jeremy Benthan no final do século XVIII, que fora reapresentada por Michel Foucault, em 1979[13]. O modelo panóptico de Bentham orientava a construção de um anel periférico, dividido em celas, cada uma ocupando toda a largura da construção. As salas teriam duas janelas; uma abrindo-se para o interior; outra para o exterior, permitindo que a luz atrevesse a cela de um lado para o outro. Dessa forma, bastaria colocar um vigia na torre central e, em cada cela colocar um louco, um doente ou condenado (FOUCAULT, 1979, p. 210).

[13] O modelo panóptico foi apresentado como uma arquitetura vista por Benthan ao visitar a Escola Militar em Paris, em 1751, em que os dormitórios eram envidraçados, o que permitia que os alunos fossem vigiados, inclusive a noite, com o objetivo de evitar qualquer contato entre colegas (FOUCAULT, 1979, p. 211).

Nesse modelo de vigilância percebe-se o elevado sofrimento dos encarcerados, não só pelo confinamento, mas também pelo fato de saberem que estão sob permanente exposição. Ainda que o indivíduo não esteja, de fato, sendo observado, a estrutura panóptica lhe dá a impressão de que está sempre sob o olhar do vigilante.

A vigilância passou a ser utilizada como instrumento de poder pelo Estado, assim como pelas empresas privadas, formando-se uma completa rede de controle em volta da sociedade. Com as inovações tecnológicas, sobretudo na área informacional, as pessoas estão expostas a uma visibilidade permanente, à semelhança do que ocorre nas estruturas panópticas. Além da permanente observação ou sensação de exposição, os indivíduos também estão sendo classificados. Elaboram-se verdadeiros perfis para as pessoas, contendo informações detalhadas acerca das suas características, sem contar que, com a soma destas informações, pode-se construir um perfil falso, revelando-se ainda muito mais grave. Dessa forma, no atual cenário social, político e econômico, a informação constitui a matéria prima utilizada pela tecnologia para os indivíduos.

A igreja e a família foram consideradas os primeiros maiores centros catalizadores de informação, na medida em que coletavam dados pessoais a respeito das pessoas e/ou comunidades que ameaçavam o seu poderio, para depois os repassar ao controle do Estado.

Atualmente, a criação de arquivos pessoais não é mais um privilégio da igreja e do Estado, pois empresas privadas coletam informações muitas vezes de forma não autorizada para depois cruzarem estes dados com as compilações organizadas por outras empresas, como instituições financeiras, operadores de telecomunicações, internet, etc, criando-se verdadeiros perfis pessoais de consumidores.

A informação se destaca do seu conteúdo histórico para ressaltar os aspectos relacionados á manipulação, à coleta e ao tratamento de dados, considerando que a revolução tecnológica

possibilitou o incremento da capacidade de armazenamento e comunicação de informações.

O *ciberespaço* é a nova fronteira para a coleta de informações pessoais e, o seu poder só está começando, considerando que a internet está se tornando um centro de negócios de informações pessoais, isto porque fez com que o tráfico e aquisição de dados se tornassem mais fáceis (SOLOVE, 2004, p. 467)[14]. Através da internet, as pessoas estão celebrando os mais diversos contratos com outros indivíduos, localizados nos mais diferentes lugares. Basta acessar um determinado *site* de compras que, ao fazer seu cadastro, seus dados ficam armazenados, por intermédio de um programa chamado de *Cookies.*[15]

Há bancos de dados nos EUA que compilam dados sobre idade, renda, gênero, crianças e o acesso à internet. Existem ainda, bancos de dados específicos sobre a idade de crianças. Pode-se encontrar uma lista chamada *Savvy Single Womem,* que afirma que as mulheres solteiras representam um mercado importante para viagens de férias, clubes de fidelidade, cartões de credito, investimento e entretenimentos (SOLOVE, 2004, p. 481. Ebook).

Vê-se que as informações passaram a ter uma maior utilidade, tornando-se um elemento fundamental e, com isso, aumentando as possibilidades de influir no cotidiano das pessoas, no entanto, também possibilitando os excessos, o que poderá resultar justamente em um apelo à privacidade.

Como foi dito acima, a informação é expressão que pode ser analisada sob diversos aspectos, fazendo-se uma verdadeira representação da estrutura social, como por exemplo, a liberdade de expressão e comunicação, a caracterização como bem jurídico, o direito à informação, a propriedade dos meios de comunicação.

---

[14] O referido autor cita como exemplo, o s*ite Focus,* nos EUA, que se vangloria em ter informações sobre mais de duzentos milhões de pessoas.

[15] *Cookies* são arquivos de computador de armazenamento de dados para personalizar e otimizar a experiência do usuário em um determinado s*ite.* São instalados automaticamente do disco rígido do usuário no momento da visita em uma página da internet (FOROUZAN, 2006, p. 854).

Cada um desses enfoques não deve ser tratado isoladamente, isto porque na opinião de Doneda (2006, p. 154) o problema da informação não é somente complexo, é integrado. Não se pode desconsiderar os focos de tensão entre os interesses conflitantes nas diversas situações jurídicas que envolvem a informação, como por exemplo, quando se utilizam as redes sociais como exercício da liberdade de expressão e de pensamento, mas por outro lado, se ataca a privacidade e a intimidade de alguém.

Para o presente trabalho importa a noção de informação pessoal, que é apenas uma das quatro modalidades de informação, seguindo a classificação de Catala (1983, p. 22). Dentre aquelas quatro modalidades, estariam: "a) as informações relativas às pessoas e seus patrimônios; b) as opiniões subjetivas das pessoas; c) as obras do espírito; d) as informações que se referem a descrições de fenômenos, coisas e eventos".

A necessidade de se identificar a modalidade de informação que se pretende analisar está intimamente relacionada à extensão do dano causado no caso de violação a direitos como a privacidade e a intimidade da pessoa. Uma informação que possui um vínculo objetivo com determinado individuo, revelando suas ações ou características, pode ser utilizada de maneira não autorizada ou para outra finalidade devastadora à noção de privacidade.

Catala (1983, p. 20) observa que não importa que a pessoa não seja a autora da informação, no sentido de sua concepção, isto porque ela é titular legitima dos seus elementos, tendo vínculo muito estreito com o indivíduo e por esta razão merece urgente tutela.

Nos últimos anos, percebe-se que as discussões teóricas acerca da noção de privacidade demonstram que é um conceito fortemente dinâmico, em que sofreu mudanças pela chamada tecnologia de informação, bem como também pelas tecnologias de reprodução e engenharia genética.

É possível que essa tendência em mudanças na noção de privacidade prossiga nos próximos anos, acompanhando a própria evolução social. Rodotá (2008, p. 92-93) lembra que houve

também uma ampliação do próprio conceito de esfera privada, compreendendo hoje situações e interesses antes excluídos de proteção jurídica específica.

Dessa forma, pode-se identificar duas tendências: a primeira, como sendo uma redefinição do conceito de privacidade, indo além do tradicional poder de exclusão, atribuindo relevância ao poder de controle. De outro lado, o objeto do direito à privacidade amplia-se, compreendendo um número crescente de situações juridicamente relevantes.

A preocupação com a tutela da privacidade nunca foi tão grande, mostrando-se a crescer ainda mais no futuro, na medida em que as violações perpetradas contra ela atinjam uma maior camada da população, bem como considerando que as pessoas passam a perceber nas situações mais corriqueiras uma hipótese de afronta à sua privacidade.

Em meio a uma verdadeira revolução digital, nem todas as pessoas perceberam todas as suas implicações (SOLOVE, 2004, p. 133). Na década passada, testemunhou-se uma transformação dramática no que diz respeito a compras, aos serviços dos bancos e a outros negócios na vida diária das pessoas. Isso resultou no aumento, sem precedentes, de registros e dados, pois os pequenos detalhes que antes eram capturados em folhas de papel passaram a ser armazenadas para sempre nas mentes digitais.

Essa revolução digital acabou exterminando as barreiras geográficas e modificando sobremaneira o comportamento humano. As pessoas estão cada vez mais conectadas, registrando acontecimentos *in loco,* com câmaras de aparelhos celulares e compartilhando imediatamente via i*nternet,* vídeos, fotos, imagens e informações nas redes sociais.

Essa evolução nas tecnologias de informação e comunicação culminou com o aparecimento de problemas específicos que apelam por uma regulação jurídica (GONÇALVES, 2003, p. 19-20). Tais problemas, num primeiro momento, foram caracterizados pelo crescimento do poder de processamento dos computadores e

da sua capacidade de acumulação, o que orientou a proteção dos interesses econômicos emergentes em torno da informação.

Esta proteção encontrou expressão, especialmente, na formulação de direitos sobre a informação, nos regimes de proteção dos dados pessoais informatizados e na regulação do acesso e transmissão de informação administrativa. Entretanto, num segundo momento, foi marcado pelo desenvolvimento da internet.

A partir dos anos 90, a expressão preferida para representar esse novo direito emergente foi "direito da informática", no entanto, mais tarde a preferência pareceu orientar-se para um "direito da sociedade da informação", que envolve tanto o direito da era da informática, como também o direito das redes globais (GONÇALVES, 2003, p.20).

O direito da informação seria um conjunto de normas e princípios jurídicos, cujo objeto são as relações jurídicas geradas em torno da utilização das novas tecnologias da informação e comunicação para o recolhimento, processamento e transmissão da informação. A evolução tecnológica contribuiu decisivamente para valorizar a informação como bem econômico e social, bem como a comunicação como valor coletivo e individual (GONÇALVES, 2003, p. 22).

Ao tratar sobre este novo arranjo de sociedade: a sociedade da informação, Ascensão (2002, p. 71) ensina que melhor seria falar em sociedade de comunicação, em vez de informação, considerando que o que se pretende impulsionar é a comunicação, advertindo que somente num sentido muito amplo é que se poderia qualificar toda mensagem como informação.

O fato é que neste novo perfil de sociedade, a realidade foi modificada, isto porque anteriormente poderia se impedir, por exemplo, que jornais ou revistas fossem as bancas quando violadoras da privacidade e da intimidade de alguém. No entanto, hoje mostra-se como impossível tal tentativa, considerando que a informação digital alcança todos os usuários da *internet,* disseminando-se rapidamente.

No Brasil, entende-se que a internet se dividiu em dois setores: o primeiro, fortemente comercializado, onde são encontradas as empresas com fins lucrativos, inclusive livrarias e lojas de música. No segundo setor, encontram-se as ofertas gratuitas de órgãos governamentais[16] e da administração pública, universidades, associações e outros (GERMAN, 2000, p. 57).

Por meio de uma rápida análise, percebe-se um avanço das *homepages* no Brasil, uma grande criatividade e capacidade de inovação das empresas informatizadas. Os brasileiros têm facilidade de lidar com novas técnicas de forma mais pragmática e sem preconceitos, talvez, até mesmo, pelo entusiasmo causado pela nova tecnologia.

Siviero e Castro (2012, p. 55) lembram que a internet e os motores de busca permitiram a localização com grande eficiência das mais variadas informações sobre pessoas e acerca dos mais variados temas, o que culminou com incômodos para essas pessoas que não desejam que certas informações relativas a si sejam localizáveis. Pode-se citar como exemplo, o *site* do *google,* no qual podem ser encontradas pessoas, endereços ou quaisquer tipos de informação acerca das mais variadas temáticas.

Fazendo-se uma comparação da era da informação com a era industrial, pode-se perceber que se a tecnologia da informação é hoje o que a eletricidade foi para a era industrial, a internet poderia ser comparada tanto a uma rede elétrica quanto ao motor elétrico, considerando a sua capacidade em distribuir força da informação por todo domínio da atividade humana (CASTELLS, 2003, p. 07).

Ao tratar dos efeitos das modernas tecnologias de informação e comunicação na politica, economia e sociedade nos países industrializados e em desenvolvimento, German (2000, p. 13) destaca que somente os países que têm acesso a essas tecnologias estão à altura dos desafios do século XXI. Na verdade, vive-se uma

[16] Exemplifica-se com os *sites* eletrônicos <www.planalto.gov.br > e <www.dominiopublico.gov.br.>

evolução da sociedade industrial para sociedade informatizada, onde tal transformação ocorre com uma velocidade incalculável.

German (2000, p. 15) lembra ainda que, na sociedade informatizada pós-industrial, a produção do conhecimento pela pesquisa e pelo desenvolvimento, o aproveitamento desse *Know-how,* bem como, a implementação em produtos e serviços ocupam o primeiro plano. Na sociedade informatizada, a produção de materiais necessários para a vida cotidiana cede lugar para os códigos desmaterializados e digitais, como o arquivo de informações em um computador, ou mesmo um banco de dados digital. Os *softwares* tornam-se um símbolo da economia da informação.

Assim, observa-se que as novas tecnologias invadiram a vida cotidiana das pessoas com força cada vez maior e de forma altamente despercebida. Atualmente, cada cidadão do mundo ocidental utiliza em média cerca de 200 *chips* que estão instalados em eletrodomésticos, automóveis, equipamentos de escritórios e, em alguns casos se encontram implantados no corpo das pessoas, por indicação médica (GERMAN, 2000, p. 16).

Insta destacar que o início da era da informação se deu nos EUA e no Japão, e posteriormente juntaram-se a eles Londres, Paris e Frankfurt, bem como São Paulo e Bangalore. No entanto, os Estados Unidos que assumiram a dianteira tecnológica no registro, armazenamento, processamento e na transmissão de informações tinha concentrado cerca de 80% de todas as informações em bancos de dados, entretanto, percebia-se que não havia uma disposição em partilhar com parceiros da Europa ocidental esse conhecimento e a dianteira na tecnologia da comunicação (GERMAN, 2000, p. 17).

O Brasil se inseriu nessa sociedade de informação pela elaboração em agosto de 2.000 do Livro Verde da Sociedade da Informação[17], com o objetivo de assegurar que os benefícios desta

[17] Sociedade da Informação no Brasil – Livro Verde foi Publicado pelo Ministério da Ciência e Tecnologia, em setembro de 2000. Disponível em: <http://www.mct.gov.br/index.php/content/view//18878.html. Acesso em: 23 de abr. de 2014.

nova sociedade alcancem a todos os brasileiros. Este documento observa que a sociedade da informação é o fundamento de novas formas de organização e de produção em escala mundial, redefinindo a inserção de países na sociedade internacional. A sociedade da informação, segundo o documento citado, é definida como uma nova era, na qual a informação passa a ser o centro e a adquirir velocidade em quantidades inimagináveis, assumindo valores sociais e econômicos fundamentais.

Esse processo de inserção do Brasil na sociedade da informação passou por algumas etapas ou fases. A primeira delas possibilitou a representação e processamento de qualquer informação pela via digital, tendo profundas implicações no processo de globalização da economia. A segunda fase proporcionou uma queda nos preços dos computadores, nos insumos tecnológicos e programas de computadores, possibilitando um maior acesso à rede. Contudo, sabe-se que uma grande parcela da população não tem acesso a esta nova tecnologia, até mesmo por questões de ordem econômica e social.

Nesse contexto, a transformação ocorrida recentemente nas sociedades contemporâneas, retratando uma verdadeira revolução digital, com a redução das fronteiras entre as telecomunicações e os meios de comunicação em massa passou a ser denominada de sociedade da informação.

O Livro Verde da Sociedade da Informação deixa claro que o caminho rumo à sociedade da informação é repleto de desafios em todos os países, não somente no Brasil. Em cada país, o desafio reflete uma combinação de oportunidades e riscos, em que cada um terá que encontrar sua rota e suas prioridades, considerando as características da sociedade na qual está inserido (BRASIL, 2000).

Nesse sentido, causa preocupação a Lei Geral de Proteção de Dados Pessoais no que se refere à influência exercida pela Diretiva 95/46/CE, do Conselho da União Europeia. Essa diretiva europeia serviu de base para elaboração de várias legislações sobre proteção

de dados, bem como também influenciou a elaboração da legislação brasileira acerca deste tema.

No entanto, sabe-se que o Brasil tem características próprias de um país ainda em desenvolvimento, marcado por imensa desigualdade social, concentração de riquezas nas mãos de poucos, analfabetismo e um histórico de corrupção. A questão é saber se de fato, a fórmula estabelecida pelos países na União Europeia quanto à proteção de dados pessoais pode ser implementada no Brasil, considerando as peculiaridades dos aspectos sociais, econômicos e culturais, o que será aprofundado no último capítulo.

Talvez, o mais adequado e coerente seria amoldar o direito em frente às inovações tecnológicas, já que há uma necessidade premente em se regulamentar tais condutas, advindas desta nova realidade, lembrando que muitos autores entendem não ser necessária a positivação dos direitos da chamada sociedade da informação, podendo-se utilizar os diplomas já existentes, como a Constituição Federal, Código Civil, Código Penal e Código de Defesa do Consumidor. Todavia, defende-se neste trabalho, a indispensabilidade de uma legislação de proteção de dados pessoais no Brasil, como condição para concretização de direitos ligados a personalidade humana, como a privacidade e a intimidade.

Merece destaque que, após a publicação do Livro Verde da Sociedade da Informação, pelo Ministério de Ciência e Tecnologia, podem-se encontrar algumas leis que tratam de temáticas relacionadas à Sociedade da Informação, a exemplo da Lei n. 11. 419, de dezembro de 2006, que dispõe sobre a informatização do processo digital, e da Lei n. 11.900, de janeiro de 2009, que prevê a realização de interrogatórios e outros atos processuais por videoconferência.

Com relação especificamente ao uso da internet, é importante destacar a Lei n. 12.965/2014, que recentemente entrou em vigor. Conhecida popularmente como *Marco Civil* que estabelece os princípios, as garantias, os direitos e os deveres relacionados ao uso da internet no Brasil. Na fase de elaboração, o projeto que resultou

nesta importante legislação foi objeto de consulta pública *on-line*. Posteriormente o texto-base do projeto foi reapresentado, recebendo centenas de contribuições e manifestações.

Discute-se se o Marco Civil da Internet já não teria tratado satisfatoriamente da questão relativa à proteção de dados pessoais. A resposta é negativa, isto porque a citada lei tem como objetivo principal o uso da internet, fixando-se direitos e deveres dos usuários, no entanto, na parte que trata de proteção de dados pessoais, o faz de forma bem tímida, até porque não é este o seu foco principal, deixando ainda uma lacuna muito grande no que se refere a esta temática e, consequentemente merecendo proteção legal especifica, pelas razões que aqui já foram expostas. Entretanto, considera-se importante a iniciativa do Marco Civil da Internet, tendo em vista que as informações pessoais são tratadas e manipuladas por intermédio de uma rede de computadores.

Entende-se que não se pode restringir o controle sobre a informação apenas na fase de obtenção destes dados, mas também alcançá-lo em situações ulteriores. Mesmo que a informação saia do âmbito do "segredo", a pessoa continua a exercer o controle sobre sua destinação.

Se uma pessoa, ao contratar a compra de um bem durável, transmite seus dados pessoais para realização de cadastro, não quer dizer que a empresa com a qual esteja contratando poderá posteriormente se utilizar das informações coletadas para outros fins, transmitindo-as a terceiros. Nesse momento, entra em discussão a questão da autorização do titular de informações a seu respeito.

O controle é intimamente ligado à autorização ou consentimento do uso da informação, tendo em vista que só haverá controle se houver autorização. Dessa forma, o indivíduo terá liberdade de escolha na construção de sua esfera pessoal e, consequentemente, no desenvolvimento da sua personalidade.

Quanto ao consentimento ou autorização, Pinto (2002, p. 33), que prefere tratar como limitação voluntária do direito à reserva, entende que o consentimento, acordo ou autorização deve

ser considerado como limitativo do próprio direito e não como causa de justificação para a violação deste. A limitação voluntária traduz uma forma de exercício do direito à reserva sobre a intimidade da vida privada.

O acordo ou consentimento para limitação voluntária, como toda declaração de consentimento pode ser conferida expressa ou tacitamente, não necessitando que seja por escrito, considerando que no nosso direito a forma é livre, salvo nos casos em que a lei exige uma formalidade especial, conforme o Código Civil brasileiro.

Entretanto, podem surgir dúvidas acerca do consentimento tácito, o que deverá ser solucionado pelo emprego dos métodos de interpretação dos contratos, utilizando-se a boa fé objetiva e a função social do contrato como princípios norteadores da interpretação contratual.

Deve-se dar maior atenção à integridade do consentimento, uma vez que, sobretudo em situações de necessidade ou simplesmente inferioridade de poder econômico do titular do direito, as pessoas podem ser levadas a autorizar por temerem as consequências de uma eventual recusa (PINTO, 2002, p. 37). Pode-se citar como exemplo, o instituto da lesão, previsto no art. 157 do Código Civil brasileiro que dispõe que "Ocorre a lesão quando uma pessoa, sob premente necessidade, ou por inexperiência se obriga a uma prestação manifestamente desproporcional ao valor da prestação oposta"(BRASIL, 2002).

Insta observar que a declaração de limitação voluntária pode ser anulada ou ser objeto de declaração de nulidade, com fundamento em regras sobre incapacidade ou vícios de vontade. Em outro sentido, a autorização deve ser especifica para uma determinada finalidade, sendo necessária nova autorização para publicação, por exemplo, de novos acontecimentos, fatos ou aspectos, mesmo relacionados com a autorização anterior.

O direito à reserva sobre a intimidade da vida privada, expressão utilizada pelo direito português, não é indisponível, conforme a legislação portuguesa, considerando que a sua limitação

não é vedada por lei. Todavia, no direito brasileiro, o Código Civil, no seu art. 11 estabelece que os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária, salvo nos casos previstos em lei.

Entretanto, Moraes (2010, p. 125) adverte que o mencionado dispositivo do Código Civil brasileiro não deve ser interpretado na sua literalidade, pois vem sendo periodicamente temperado pela doutrina civilista, nas Jornadas de Direito Civil, promovidas pelo Centro de Estudos Judiciários da Justiça Federal. Logo na primeira jornada, realizada em 2002 foi aprovado o Enunciado n°139, que dispõe: "Os direitos da personalidade podem sofrer limitações, ainda que não especificamente previstas na lei, não podendo ser exercidos com abuso de direito do seu titular, contrariando a boa-fé objetiva e aos bons costumes".

Muito embora se saiba que a informação só possa ser transmitida a terceiros com o consentimento e autorização do seu titular, existem situações em que a cessão da informação é imprescindível e, por este motivo, pretende-se analisar as hipóteses em que a transmissão de informações é indispensável na seção subsequente.

2.4 Cogência da cessão da informação e a necessidade de proteção.

No tópico anterior foi exaustivamente discutida a importância da informação na vida das pessoas da sociedade moderna e, mais ainda, a proporção que a informação tomou com o surgimento dos computadores e da internet. Como afirma Marques (1975, p 13), o computador excitou a imaginação das pessoas, gerando grandes esperanças e receios. Assim, como as faces de Juno, o uso da internet e a massificação do acesso aos computadores interligados trouxeram bons e maus efeitos. Ao passo que permitem a aceleração do processamento e difusão das

informações, também permite o uso nocivo, como por exemplo, a facilitação de lesão à privacidade.

A privacidade e a intimidade estão constantemente ameaçadas. Todos podem estar sob a mira de câmeras ou ter seus dados armazenados e divulgados quase sem nenhum controle. Todos estão sujeitos à vigilância. As escutas telefônicas e outros meios de vigilância se ampliam continuamente, sem um severo controle judicial ou legislativo.

Os governos instalam postos secretos de observação. Empresas e indústrias instalam circuitos internos de televisão que se estendem até às suas moradias, possibilitando o acesso das imagens de qualquer lugar em que se encontre. Testes pessoais tentam extrair dos homens os pensamentos mais íntimos. Todos estes exemplos servem para comprovar que por todas as partes a intimidade, a privacidade e a dignidade dos cidadãos estão sendo restringidas (DOTTI, 1980, p. 142).

Embora todas essas situações pareçam absurdas, sob a perspectiva da proteção à intimidade e à privacidade das pessoas, há casos em que tais interesses cedem lugar ao interesse público. É possível justificar limitações à privacidade, para sobrelevar os interesses da segurança nacional, da investigação criminal; da saúde pública; da história; da crítica; da cultura e outras restrições (DOTTI, 1980, p. 140).

Cita-se o caso do romancista Alexandre Dumas que pretendia erguer um monumento em memória a Balzac, autor de *A Comédia Humana*. Como um exemplo de limitação à privacidade da viúva, que se mostrou contrária à ideia, alegando que o direito à homenagem era privilégio da família. Em 1854, o Tribunal de Sena decidiu que a edificação de um monumento em honra de um homem ilustre seria uma homenagem pública em reconhecimento ou admiração àquele que honrou seu país. Decidiu que não havia nenhum impedimento para o ato de homenagem (DOTTI, 1980, p. 141). Ainda naquela época, viu-se uma preocupação em

contrabalançar eventual conflito entre a privacidade e outros interesses relevantes.

Como os demais direitos fundamentais e de personalidade, a privacidade não ostenta caráter absoluto, está sujeito a restrições expressas ou implícitas que podem derivar da própria Constituição, como nos casos em que se prevê a suspensão do direito de reunião e do direito à privacidade em estado de defesa, conforme o § 1º, art. 136, CF/88[18]. A própria Constituição dá azo à mitigação da privacidade, representada pelo sigilo das correspondências, comunicação telegráfica e telefônica nas hipóteses imprescindíveis à defesa da segurança nacional.

É bem certo que, recorrendo-se à teoria de Alexy (2008, p.286), os direitos fundamentais só podem ser restringidos por normas de hierarquia constitucional ou normas infraconstitucionais nas hipóteses previstas pelo próprio constituinte. A privacidade também poderá sofrer restrições quando em conflito com outro direito igualmente fundamental. Nesse caso, a tensão deverá ser solucionada pela jurisprudência por meio das técnicas próprias[19].

Caso paradigmático foi julgado pelo Supremo Tribunal Federal (RCL 2.040/DF, 2002), envolvendo a mexicana Glória Trevi, que aguardava a extradição para o seu país, na carceragem da Polícia Federal. Durante a prisão, a extraditanda engravidou e deu à luz a uma criança que julgava ser fruto do abuso sexual sofrido por algum policial[20]. Determinou-se o exame de DNA

[18] "O decreto que instituir o estado de defesa determinará o tempo de sua duração, especificará as áreas a serem abrangidas e indicará, nos termos e limites da lei, as medidas coercitivas a vigorarem, dentre as seguintes: I – restrições aos direitos de: a) reunião, ainda que exercida no seio das associações; b) sigilo de correspondência; c) sigilo de comunicação telegráfica e telefônica; II – ocupação e uso temporário de bens e serviços públicos, na hipótese de calamidade pública, respondendo a União pelos danos e custos decorrentes."

[19] Na técnica adotada por Ronald Dworkin (2002, p. 41-43), quando há conflito entre princípios, o árbitro deve sopesar a força relativa de cada um deles, utilizando-se do sopesamento. Já as regras são sempre corporificadas em dispositivos legais e aplicadas à maneira do tudo-ou-nada.

[20] A extraditanda, Gloria Trevi, denunciou para a revista Isto é, edição 1677, que havia sido estuprada na carceragem da Policia Federal. Assim, o caso foi parar no Supremo Tribunal Federal, por meio de

forçado na criança para averiguar a paternidade e a isso se opôs Glória Trevi, levando o caso ao STF que denegou o seu pedido.

O STF considerou a necessidade de solução do caso pela ponderação entre o direito à intimidade e à vida privada da extraditanda e à imagem dos servidores da Polícia Federal, atingidos pela declaração falsa de que a suplicante havia sido estuprada. Optou pela proteção da imagem dos servidores federais, buscando a verdade real sobre eventual violência sexual perpetrada nas dependências da Polícia Federal.

A respeito da privacidade, como direito à autodeterminação informativa, vale a pena destacar outro caso julgado pelo Superior Tribunal de Justiça, em sede de Recurso Ordinário em Mandado de Segurança (RMS n. 15146/SC). A justiça federal havia determinado a quebra do sigilo bancário de uma pessoa, requerido pelo Ministério Público, por suspeita de crime financeiro, mas a decisão foi atacada por Mandado de Segurança, no qual foi denegada a ordem contra decisão do juízo federal.

Da denegação da segurança, foi interposto Recurso Ordinário, perante o Superior Tribunal de Justiça, que não deu provimento ao recurso por alegar que o sigilo bancário não constitui um direito absoluto, deparando-se com uma série de exceções legais ou impostas pela necessidade de defesa ou salvaguarda de interesses sociais mais relevantes (RMS n.15146/SC/2003)[21].

Não obstante saber que o direito à privacidade, como qualquer direito fundamental e da personalidade não ostenta caráter absoluto, sendo passível de sofrer restrições ou limitações,

---

Reclamação feita pela própria extraditanda, quando soube que seria feito a sua revelia e por ocasião do parto do filho, exame do liquido aminiótico para averiguação da paternidade. No caso em tela, a suplicante alegou que a paternidade do seu filho reveste-se de características atinentes a personalidade do nascituro e da intimidade da vida privada dela, posto que as consequências de eventual investigação teriam reflexos na vida de ambos. (Reclamação nº 2.040/DF/2002. Rel. Min. Néri da Silveira. Julgado em 21/02/2002. Disponível em: www.stf.gov.br. Acesso em: 25/06/2014).

[21] Recurso Ordinário em Mandado de Segurança nº 15.146/SC. Julgado em 12/03/2003. DJ 07/04/2003. Disponível em: <http://www.stj.gov.br/SCON/jurisprudencia > . Acesso em: 25/06/2014.

a sua violação, nos dias atuais, tem sido motivo de preocupação por parte de Estados e até mesmo das pessoas em geral. Nesse contexto, em dezembro de 2013, a Assembleia Geral da ONU aprovou resolução apoiando o direito à privacidade, solicitando que todos os países adotassem medidas para por fim às atividade que violem esse princípio da sociedade democrática (ONUBR, 2013).

O texto foi intitulado de "Direito à privacidade na era digital", com colaborações do Brasil e Alemanha, demonstrando a preocupação com um possível impacto negativo no que se refere à vigilância eletrônica, da interceptação de comunicações, bem como recolhimento de dados pessoais (ONUBR, 2013)[22]. O documento ressalta o direito à privacidade como um direito humano e afirma que as pessoas têm o mesmo direito quando estão *on-line* ou *of line,* ainda que reconheça a possibilidade de coleta de certas informações, por motivo de segurança pública. Reafirma que os países devem cumprir suas obrigações perante o direito internacional.

Destaca-se que a participação conjunta do Brasil e da Alemanha na elaboração dessa resolução, demonstra a preocupação com a privacidade na era digital que se acentuou após a divulgação, pela imprensa, do chamado *caso Snowden*[23]*,* um ex-funcionário da Agência de Segurança Nacional – NSA dos Estados Unidos, acusado de divulgar vários programas de vigilância eletrônica secretos para a imprensa, bem como de informar que os EUA espionavam governos, cidadãos, empresas de países aliados, ou não, inclusive o Brasil.

---

[22] Disponível em: http://www.onu.org.br. Acesso em: 01 de jul 2014.

[23] Edward Snowden foi acusado de espionagem por vazar informações sigilosas de segurança dos Estados Unidos e revelar detalhes dos programas de vigilância que o país usa para espionar a população americana e vários países da Europa e da América Latina, dentre eles, o Brasil, inclusive monitorando conversas com a Presidente Dilma Rousseff. Snowden requereu asilo a diversos países, inclusive ao Brasil, no entanto, conseguiu asilo temporário na Rússia, o que fez com que a Casa Branca tivesse ficado desapontada com a decisão daquele país. Em janeiro de 2014 a Rússia anunciou que estenderá o asilo e não o mandará de volta aos EUA, entretanto, posteriormente, Snowden disse que pretendia iniciar negociações de seu retorno ao país de origem, com a garantia de que receberia anistia. (Reportagem Disponível em: http://www.g1.globo.com, de 21/07/2013. Acesso em: 30 de jun. 2014.

Os fundamentos utilizados para elaboração da resolução sobre direito à privacidade na era digital foram: Declaração Universal dos Direitos do Homem, Pacto Internacional sobre Direitos Civis e Políticos e o Pacto Internacional sobre Direitos Econômicos, Sociais e Culturais.

Destaca-se que, somente após a divulgação de informações de que o governo e algumas empresas brasileiras estariam sendo alvo de espionagens pelos EUA, é que o governo brasileiro passou a se preocupar mais efetivamente com a proteção de dados no Brasil. Todavia, sabe-se que até 2018, o Brasil era o único do Mercosul que ainda não possuia uma legislação especifica sobre a proteção de dados pessoais, em contraposição ao que já se verifica em países como Argentina, Uruguai e Paraguai, e em alguns países que integram a União Europeia. A discussão ganha fôlego, no Brasil, com pelo menos 40 anos de atraso em relação a países europeus e aos EUA, considerando que estes também têm legislação especifica desde a década de 70[24].

Castells (2003, p. 147) observa que a primeira vitima dessa retomada de posse do *ciberespaço* é a própria soberania, isto porque para que os Estados sejam parceiros nessa rede de controle, devem concordar com padrões comuns, sendo moldados segundo um denominador comum. Explicando melhor: se um determinado Estado, por exemplo, deve cooperar, impondo controle sobre *websites* de pornografia infantil localizados em seu território, ele só o fará sob a condição de ter acesso a dados obtidos a partir da interceptação do tráfego entre os demais países.

Isso demonstra a possibilidade de ameaça à soberania, na medida em que os Estados participem dessa rede de vigilância policial, no entanto, embora se saiba que a repressão será diferenciada segundo o grau de liberdade em cada país, sua base

[24] Vale destacar que recentemente, após anos de discussão e tramitação foi aprovado em maio de 2018 no Plenário da Câmara dos Deputados o PL n. 4.060/2012, com adaptações sugeridas pelo PL 5.276/16 e encaminhado ao Senado Federal e posteriormente, após aprovação no Senado Federal, convertido na Lei 13.709/2018.

informacional será ajustada aos padrões cabíveis de suspeita compartilhados por todos os governos que participam desta rede de vigilância (CASTELLS, 2003, p. 148).

Observa-se que a vigilância global pode atingir inclusive a liberdade de expressão, uma vez que há possibilidade de o tráfego ser interceptado por agências de vários países, bem como a utilização dos dados obtidos não ficarem restritos a determinada jurisdição. Castells (2003, p. 148) cita como exemplo, o consumo legal de maconha na Holanda por um cidadão norte-americano, que pode ser exposto e reprimido nos Estados Unidos por uma vigilância conjunta sobre a distribuição de drogas.

Nesse sentido, verifica-se que além da soberania, a liberdade está constantemente ameaçada, considerando esta nova arquitetura da internet, em que a vida cotidiana das pessoas, o trabalho, o lazer e a interação pessoal têm lugar no espaço virtual, ou seja, viver num meio eletrônico significa ter a metade de nossas vidas expostas ao monitoramento.

A efetivação do direito à privacidade, em especial, no aspecto aqui discutido, como direito à autodeterminação informativa, depende de uma ação positiva por parte do Estado, com o objetivo de implementar medidas administrativas e legislativas, imprescindíveis para a concretização desse direito fundamental no estágio atual da tecnologia da informação.

3

A proteção internacional dos dados pessoais

Após as considerações acerca da conformação do direito à privacidade como direito fundamental e da personalidade, bem como acerca da sua expansão conceitual, é necessário investigar a proteção de dados pessoais no direito alienígena.

Inicialmente serão feitas algumas considerações acerca dos dados pessoais para, em seguida, contextualizar a temática no panorama internacional. Enfocar-se-á o modelo europeu, considerado paradigmático no que pertine à proteção de dados. No entanto, será analisada também a legislação italiana, que apesar de ter sido a última a normatizar esta matéria no âmbito na U.E, foi considerada paradigmática, pois representa a primeira tentativa, em escala internacional, de reordenação geral de uma matéria complexa e, sobretudo, extraordinariamente móvel. O modelo americano também será objeto de estudo, com o objetivo de demonstrar a evolução do *Right to privacy,* desde o célebre artigo de Warren e Brandeis. Eventualmente, quando se fizer necessário, far-se-á a comparação entre os modelos acima mencionados com o sistema brasileiro de proteção de dados pessoais.

3.1 Considerações acerca dos dados pessoais

A evolução na tecnologia da informática permitiu uma mudança na estrutura organizacional das empresas. Nos dias atuais, as grandes organizações empresariais empregam seus esforços de desenvolvimento em função da internet, oferecendo,

como por exemplo, as lojas virtuais, que divulgam seus produtos de forma globalizada.

Essa nova forma de organização necessita mais ainda das informações constantes em bancos de dados dos seus clientes atuais ou futuros. Todos esses bancos de dados passam a ser informatizados, por meio de uma rede de computadores interligados. Caracterizam-se como um conjunto de dados com organização e procedimentos próprios de manipulação, com o objetivo de armazenamento para posterior recuperação destes dados (MEDEIROS, 2007, p. 30).

Muito embora alguns autores façam a distinção entre os termos "dados" e "informações", como já foi anotado anteriormente no tópico 1.4., para este trabalho, as duas expressões serão consideradas como sinônimas, pois o tipo de informação que se pretende discutir aqui é aquela pessoal, referente à própria pessoa, e não outros tipos de informação[1].

Como exemplo de dado pessoal (de pessoa identificável), pode-se citar o IP, código atribuído a determinado computador quando este se conecta a uma rede. Ainda que não se possa identificar diretamente a pessoa, é possível alcançar a sua identificação a partir da interconexão do IP aliada a outros dados armazenados pelo provedor de acesso à internet[2].

A evolução na tecnologia da informática permite que as pessoas sejam catalogadas por bancos de dados informatizados, controlados por s*oftwares,* que cruzam dados e buscam informações, desde o seu nascimento até a sua morte. A título de

[1] A Directiva 95/46/CE, no seu art. 2° trata os termos "dado" e "informação" como expressões sinônimas, quando define dado pessoal: "como qualquer informação relativa a uma pessoa singular identificada ou identificável; sendo identificável aquela pessoa que possa ser identificado, direta ou indiretamente, por referência a um número de identificação ou a algum elemento especifico da sua identidade física, psíquica, econômica ou social". Disponível em: http://www.eur-lex.europa.eu. Acesso em: 09 de jul. 2014.

[2] Dado pessoal, segundo Catarina Sarmento Castro (2005, p. 70-71) é o dado relacionado a um individuo identificado ou identificável, independentemente do suporte em que se encontre registrado, se por escrito, por imagem, som ou vídeo. O indivíduo identificado é aquele já conhecido; o identificável é o individuo que pode ser conhecido diretamente pelo possuidor de seus dados.

exemplo, podem-se citar os dados inseridos no Cartório de Registro Civil, quando do nascimento de uma pessoa. Posteriormente, as suas informações passam a integrar o banco de dados da Secretaria de Segurança Pública, do órgão de Departamento de Trânsito, da Receita Federal e outros[3]. Além desses, há os bancos de dados formados pelas pessoas jurídicas de direito privado, a partir da declaração voluntária de informações por parte do respectivo titular.

As pessoas ao contratarem com agentes privados, respondem a uma série de questionários que solicitam informações pessoais, autorizando a composição de um especifico banco de dados. Muitas vezes, o consumidor interessado em uma contratação de serviços ou produtos é levado a fornecer os seus dados, sob pena de prejudicar aquela avença. Paulatinamente, suas informações vão sendo disponibilizadas ao ponto de fragilizar a sua privacidade, especialmente com o uso de recursos tecnológicos que facilitam a sua manipulação, monitoramento e, consequentemente, devassa à intimidade. Assim, percebe-se a necessidade de controle destas informações por parte de seus titulares, que muitas vezes não têm ideia dos efeitos que a coleta, armazenamento e interconexão de dados pessoais podem trazer para a sua vida privada.

Os dados pessoais podem assumir as características de dados não sensíveis, dados sensíveis e dados de tratamento proibido. Os primeiros se referem aqueles dados que podem ser compartilhados com um maior número de pessoas, correspondendo a esfera privada do indivíduo, conforme a teoria alemã dos círculos concêntricos. Já os dados sensíveis correspondem àqueles dados que são compartilhados com um número menor de pessoas, pertinentes à esfera da intimidade, cujo acesso é restrito. Os dados de tratamento proibido correspondem exatamente à esfera do

[3] Esses tipos de bancos de dados mencionados, considerados públicos cadastram informações de declaração obrigatória. Nesse aspecto, diferem dos bancos de dados formados pelas empresas privadas (estabelecimentos bancários, lojas, escolas, associações e outras). O objeto da presente tese são as informações colecionadas a partir da declaração voluntária da pessoa.

segredo e abrangem as manifestações mais íntimas do indivíduo que devem estar a salvo de qualquer devassa ou divulgação.

Observa-se que mesmo os dados não sensíveis podem causar dano à personalidade do indivíduo, necessitando assim de proteção, com o fito de garantir a sua integridade, autenticidade e confidencialidade. Isto porque tais dados, uma vez confrontados com outros, podem revelar aspectos da privacidade ou intimidade que o seu titular gostaria de manter em sigilo.

O grande problema em relação aos dados pessoais se refere àqueles denominados sensíveis, por guardarem informações de aspectos íntimos da vida da pessoa, como por exemplo, raça, cor, opções políticas, religiosas, filosóficas, sexual e àqueles atinentes à saúde e, por esta razão necessitam de autorização expressa do titular. Muitas vezes, empresas privadas e o próprio poder público se utilizam destas informações para criar verdadeiros perfis pessoais, culminando com atitudes discriminatórias por parte de quem se utiliza destes dados/perfis.

Nos dias de hoje, discutem-se as questões ligadas à bioética, mais especificamente à engenharia genética e à preservação do sigilo de dados genéticos das pessoas. Atualmente, é possível através de exames, verificar acerca da propensão de determinado paciente para contrair uma doença. Dessa forma, questiona-se se a pessoa que toma conhecimento de que é propensa a certa anomalia, deve comunicar o fato ao cônjuge, companheiro ou aos seus descendentes? Ou mesmo se os dados genéticos coletados por uma instituição de pesquisa poderiam ser divulgados para outras entidades públicas ou privadas? (VIEIRA, 2007, p. 257)

O compartilhamento de dados genéticos, mesmo com o prévio e expresso consentimento do titular pode acarretar danos não só a ele próprio, mas também a toda a sua família. Considere-se que tais informações podem ser utilizadas para outros fins, como por exemplo, para a restrição à contratação de seguros pelas seguradoras de saúde, a partir do seu patrimônio genético. Assim,

conclui-se que informações referentes a dados genéticos constituem também dados sensíveis, merecendo igual proteção.

Mesmo que as informações sobre determinada pessoa estejam corretas, ainda assim poderá haver dano ao seu titular, caso sejam divulgadas indevidamente por terceiros não autorizados e mal intencionados (VIEIRA, 2007, p. 255). Nesse sentido, muitos países têm editado legislações específicas para proteção de dados pessoais, com o objetivo de minimizar os ataques á privacidade e à intimidade do indivíduo.

Vale lembrar que a privacidade informacional ou direito à autodeterminação informativa foi reconhecida pela primeira vez pelo Tribunal Constitucional Alemão, em 15 de novembro de 1983, em decisão que declarou a inconstitucionalidade da Lei do Censo de 1983, que obrigava os cidadãos alemães a responder um questionário com informações pessoais, para fins estatísticos, bem como para formar um banco de dados e transmitir tais informações à outras entidades federais, estaduais e municipais[4].

No plano constitucional, a Constituição Portuguesa de 1976, previu a proteção aos dados pessoais, no seu art. 35:

1. Todos os cidadãos têm o direito a tomar conhecimento do que constar de registros mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a retificação dos dados e sua atualização;
2. São proibidos o acesso de terceiros a ficheiros com dados pessoais e a respcctiva interconexão, bem como os fluxos de dados transfronteiras, salvo casos excepcionais previstos em lei.

[4] Na sentença da Corte Constitucional Alemã foi feita uma profunda consideração a respeito da proteção constitucional da personalidade, em frente aos riscos da informática, principalmente no que diz respeito à coleta e tratamento de informações pessoais que estariam a exigir a definição de critérios a ser utilizados na conformação do exercício do poder estatal de realizar um censo para fins estatísticos e administrativos, com as restrições impostas à proteção da personalidade (SAMPAIO, 1998, p. 476).

3. A informática não pode ser utilizada para tratamento de dados referentes à convicções filosófica ou políticas, filiação partidária ou sindical, fé religiosa ou vida privada, salvo quando se trate do processamento de dados estatais não individualmente identificáveis.
4. A lei define o conceito de dados pessoais.
5. É proibida a atribuição de um número nacional único aos cidadãos. (PORTUGUAL, 1976)

Após a previsão acerca da proteção de dados pessoais pela Constituição Portuguesa, sobretudo em relação ao uso da informática, outras Constituições também passaram a tratar do assunto, a exemplo da Constituição espanhola, que estabeleceu a limitação do uso da informática para garantir a honra e a intimidade pessoal e familiar, assim como outras constituições europeias tiveram a mesma iniciativa, como a da Hungria de 1989 e, da Suécia de 1990.

No Brasil, como já foi referido, a Carta de 1988 trouxe uma técnica, considerada moderna na proteção da intimidade. O inciso X, do art. 5º previu a inviolabilidade da intimidade e da vida privada, de uma forma bastante ampla e genérica e, posteriormente, no inciso XII, dispôs sobre a inviolabilidade de dados.

Argumenta-se: seria de fato necessária a regulamentação por legislação específica de proteção de dados pessoais, considerando as leis já existentes em matéria de proteção da intimidade e da vida privada? O direito à autodeterminação informativa deve ser considerado não só como um viés do direito à privacidade, mas também como um direito autônomo?

Este direito deve ser analisado no contexto atual desta nova era tecnológica, na qual a informação é um elemento imprescindível, mas que merece tutela efetiva, quando se trata de informações pessoais, atributos da própria personalidade da pessoa humana.

Nesse trabalho, defende-se a importância de lei específica para a proteção de dados pessoais, estabelecendo-se um conjunto

normativo adequado à proteção da chamada privacidade informacional. O Estado precisa implementar medidas administrativas para proteção de dados pessoais tanto para o setor público como para o privado, medidas estas que serão discutidas no último capítulo deste trabalho, quando se fará análise crítico-reflexiva acerca dos projetos de leis de proteção de dados pessoais no Brasil.

A regulamentação acerca da proteção de dados pessoais é uma tendência já concretizada em diversos países da Europa e América Latina. O Brasil apresentava até 2018 uma grande lacuna no que se refere à disciplina da privacidade informacional, fato recentemente reafirmado, quando se soube que o governo brasileiro, bem como cidadãos e determinadas empresas estavam sendo espionadas pelos EUA[5].

No entanto, para melhor compreensão do panorama internacional de proteção de dados pessoais, faz-se necessário analisar os principais modelos de proteção de dados, sobretudo o europeu que serviu de exemplo para a edição de várias legislações específicas de proteção à privacidade informacional.

3.2 A proteção de dados pessoais na União Europeia

Pelas razões já consideradas, a formação de bancos de dados tem sido uma preocupação constante dos Estados modernos. Em face disto, visando à garantia do direito à privacidade informacional, surgiram as primeiras iniciativas legislativas para a utilização e tutela desses dados. Em 1970, a Alemanha promulgou a Lei do *Land* alemão de Hesse (1995) para regular os bancos de dados informatizados de dados governamentais. A referida lei criou uma autoridade ou comissário para a proteção de dados, encarregado do controle e elaboração informática dos dados pessoais no confronto com a

[5] Caso *Snowden* citado no tópico 2.4. Reportagem Disponível em: http://www.g1.globo.com, de 21/07/2013. Acesso em: 30 de jun. 2014.

administração pública (SAMPAIO, 1998, p. 481). Em 1973, a Suécia elaborou o Estatuto para bancos de dados – *Data Legen 289 ou Datalag,* que também criou um inspetor – o *Dataispektionen,* para controlar o uso de dados pessoais.

Essas leis foram as primeiras normas a despontar uma preocupação com a coleta indiscriminada e não autorizada de dados pessoais, razão pela qual foram classificadas como leis de primeira geração no trato da questão (RODOTÁ, 1995, p. 45). Tais normatizações tinham como núcleo, a concessão de autorizações para a criação dos bancos de dados e o seu controle posterior pelos órgãos públicos.

Nas chamadas leis de primeira geração, identificam-se as seguintes características: a) tratava-se de uma legislação garantista, situada na linha histórica das declarações de direitos; b) de conteúdo amplo e pretensamente uniforme para todas as situações; c) o instrumento jurídico principal era a autorização, a partir de uma autorização prévia para seu funcionamento, acompanhada de um controle por parte de órgão institucional; e d) de aplicação restrita das pessoas físicas (SAMPAIO, 1998, p. 490).

Em virtude da amplitude do texto e da pretensão de apresentar uma solução uniforme para todas as situações de violação da privacidade, a legislação de primeira geração deixou a desejar em alguns aspectos. Ademais, observou-se que os bancos de dados não se mostraram tão perigosos, quanto supunham os legisladores. Na maioria, continham informações pessoais que seriam pouco relevantes à intimidade, como por exemplo, o endereço e telefones de clientes. Também se verificou que era impraticável o regime de autorização previsto nas referidas leis, surgindo a necessidade na elaboração das leis de segunda geração.

Com a multiplicação de centros de processamento de dados, as referidas leis de primeira geração acabaram sendo consideradas ultrapassadas, tornando ineficaz um controle baseado em um regime de autorização rígido que demandava um minucioso acompanhamento (DONEDA, 2006, p. 209). Estas normas que

estabeleciam o funcionamento dos bancos de dados não conseguiram acompanhar a sua expansão.

As chamadas leis de segunda geração caracterizavam-se por apresentar um maior aprofundamento doutrinário, com um maior grau de definição dos seus institutos. Estabeleceram os princípios de boas práticas informáticas que deveriam ser seguidos pelos centros processadores e simplificam os procedimentos exigidos para instalação e operação destes centros, mitigando o princípio da autorização ou o substituindo pelo modelo de registro (SAMPAIO, 1998, p. 491).

A preocupação das leis acima mencionadas não era mais com o sistema computacional em si, mas na consideração da privacidade e na proteção de dados pessoais como uma liberdade negativa, a ser exercida pelo cidadão. Pode-se citar como exemplo desta geração de leis, as Constituições portuguesa e espanhola. Pretendiam criar um sistema que fornecesse instrumentos para o cidadão identificar o uso indevido de suas informações.

As leis de terceira geração, surgidas em 1980 ressaltaram a necessidade de uma ampla reflexão crítica sobre a adequação dos modelos e dos instrumentos de tutela até então adotados, especialmente considerando as severas críticas que os setores sociais dirigiram a legislação anterior, por conta da sua pouca flexibilidade.

Também foram objeto de reflexão, os relatórios produzidos pelos órgãos de controle, assim como também as pesquisas patrocinadas pela Comissão da Comunidade Europeia acerca do impacto das leis sobre o setor terciário. Não ficou de fora igualmente, a reflexão sobre as consequências das novas tecnologias, com o desenvolvimento dos sistemas de informática em redes.

Os impactos produzidos pelas novas técnicas de informação foram importantes na redefinição do conceito de privacidade e intimidade para além de sua identificação com posturas isolacionistas, próprias do pensamento individualista do final do

século passado. A ideia é a de que a tutela da privacidade deve-se efetivar de forma mais ampla, abrangendo a proteção de dados pessoais, como parte integrante da personalidade humana.

Assim, as leis de terceira geração, passaram a ter preocupação com a tutela dos dados pessoais, concentrando-se no cidadão, entretanto, abrangendo muito mais do que a simples liberdade de fornecer os seus dados pessoais, mas também garantindo a efetividade desta liberdade. Doneda (2006, p. 211) esclarece que a proteção de dados pessoais é um processo mais complexo, que envolve a participação do indivíduo na sociedade e leva em consideração o contexto no qual os dados são solicitados, como forma de proteção para as ocasiões em que a liberdade é cerceada.

Dessa forma, a participação do indivíduo nas leis de terceira geração fazia parte da sua estrutura. Todavia, nem todas as pessoas estariam dispostas a exercitar seu direito à autodeterminação informativa, seja por conta dos custos envolvidos, seja porque não tinham nem mesmo conhecimento sobre o uso dessas informações. Assim, a liberdade informacional continuava sendo um privilégio de uma minoria, que arcava com os custos desta proteção.

As leis existentes atualmente em diversos países são classificadas como de quarta geração. Caracterizam-se por suprir as desvantagens do enfoque estritamente individual proposto pela legislação antecedente. Nestas, percebe-se que a tutela dos dados pessoais não pode ser efetivada pela exclusiva atuação individual do titular. São necessários novos instrumentos que elevem o padrão coletivo de proteção na busca de resultados concretos (DONEDA, 2006, p. 212).

Tais leis procuraram fortalecer a posição da pessoa em face das entidades de coleta e processamento de dados, reconhecendo-se o desequilíbrio desta relação, que não se reestabelece somente pelo reconhecimento do direito à autodeterminação informativa. Em muitos casos, necessita-se de uma proteção mais ampla e

cuidadosa, especialmente no que toca à coleta, armazenamento e manipulação dos dados sensíveis.

Não há dúvidas de que tanto a Lei de Hesse, em 1970, como a Lei sueca de 1973, influenciaram o debate em outros países acerca da proteção de dados pessoais. A primeira influenciou o relatório do Departamento de Saúde, Educação e Bem-Estar norte-americano.

Na oportunidade, descartou-se o modelo advindo da lei de 1970, pois a comissão que elaborou o relatório entendeu que a referida lei destinava-se mais a proteger a integridade dos dados armazenados pelo governo, do que propriamente tutelar interesses do cidadão. Já a Lei sueca, despertou maior interesse dos estudiosos, de sorte que vários enviados governamentais e não governamentais europeus e de outros países visitaram Estocolmo para conhecer a experiência dela decorrente (SAMPAIO, 1998, p. 499).

O fato é que, quando se vive em meio à globalização, a experiência de um determinado país pode servir como parâmetro para outro Estado, desde que haja adaptações à realidade local. É exatamente nesse ponto que a Lei Geral de Proteção de Dados Pessoais, recém aprovada no Brasil suscita preocupação. Conforme se analisará no ultimo capítulo deste trabalho, a referida legislação foi absolutamente influenciada pela legislação europeia, mais especificamente pela Diretiva 95/46/CE e pelo Regulamento Geral de Proteção de Dados Pessoais da União Europeia, que entrou em vigor em setembro de 2018, sem que fossem consideradas as particularidades nacionais.

Por conta dos riscos decorrentes da influência da legislação de um país sobre o outro, no que toca à proteção de dados pessoais, diversos organismos internacionais passaram a defender a necessidade de construção de um regime mais eficaz de tutela dos dados pessoais, sugerindo um ambiente uniforme de regulação das técnicas informáticas. A esse respeito, destaca o Conselho da Europa e a Organização para Cooperação e Desenvolvimento Econômico – OCDE.

3.2.1 Desenvolvimento do modelo europeu

O modelo europeu estrutura-se em torno de uma Diretiva, instrumento normativo da União Europeia, que tem como função básica, uniformizar a legislação. Quando este documento é aprovado, cada país-membro deve adequar, dentro de certo período, sua legislação aos moldes estabelecidos por este documento.

A legislação efetivamente aplicada aos casos concretos é a nacional, resultante da transposição da Diretiva pelos Estados-membros que compõem a União Europeia. Somente excepcionalmente se aplica diretamente a própria Diretiva, como na hipótese de o Estado ainda não possuir legislação aplicável ao caso.

Dessa forma, a proteção de dados pessoais na União Europeia foi unificada durante muito tempo em torno da Diretiva 95/46/CE[6], que se refere à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, bem como a Diretiva 2002/58/CE, relativa à privacidade e as comunicações eletrônicas, que serão analisadas mais à frente.

O sistema de proteção de dados pessoais, baseado nas respectivas Diretivas representa um padrão mínimo de proteção em toda a União Europeia, tendo como base a experiência de alguns países europeus que já haviam legislado. Observa-se que os Estados-membros que compõem este bloco, ao efetivarem a transposição da Diretiva às legislações nacionais podem modificar seu conteúdo em alguns aspectos acessórios ou nos pontos que estiverem autorizados a fazê-lo.

[6] Em 2016, a Directiva 95/46/CE foi revogada pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, que pretendeu unificar toda a regulamentação acerca da proteção de dados pessoais na União Europeia. Um dos objetivos do Regulamento é a harmonização Legislativa, passando a existir um único documento legal sobre Proteção de Dados Pessoais em todos os vinte oito Estados Membros.

Como foi mencionado no tópico anterior – 3.2, a primeira Lei de Proteção de dados pessoais foi a Lei do *Land* de Hesse, em 1970, disciplinando os centros de processamentos de dados do poder público e, instituindo pela primeira vez a figura do comissário para a proteção de dados pessoais.

No entanto, a primeira lei nacional foi a Lei sueca, de 1973, isto porque a lei alemã era apenas de um *Land* (Estado). Posteriormente, em 1978, surgiu a Lei 78 na França, denominada *Informatique et des Libertés,* instituindo-se um órgão chamado de *Comission Nationale de I'Informatique et des Libertés,* encarregado de zelar pela sua aplicação.

Todas as legislações nacionais foram criadas em meio a um ambiente no qual se demonstrava a preocupação de criar uma solução comum para o problema da proteção de dados pessoais. Nesse sentido, o Conselho da Europa, criado em 1948 com a finalidade precípua de promover a colaboração entre os diversos países democráticos europeus, na defesa do Estado de Direito e no respeito aos direitos humanos, resolveu adotar algumas recomendações no que se refere a este novo fenômeno de coleta de informações.

Inicialmente, a Assembleia parlamentar, órgão consultivo do Conselho da Europa adotou uma recomendação de número 509/68, que sugeria ao Comitê de Ministros a criação de comissão de estudos sobre direitos humanos e tecnologia em 1968, com o objetivo de saber se a proteção oferecida pela Convenção Europeia de Direitos Humanos era adequada para enfrentar as evoluções das técnicas mais modernas.

Como o trabalho não levou a conclusões satisfatórias, dividiram-se em duas fases: a primeira teve como objetivo a análise dos centros eletrônicos de dados do setor privado e resultou na Resolução nº 73, de 22/09/73, prevendo os princípios da boa-fé e pertinência na coleta de dados, bem como seu uso somente para o fim determinado (SAMPAIO, 1998, p. 502-503).

A Resolução n. 73 incentivava os países europeus a adotarem princípios mínimos pertinentes à proteção de dados, visando a uma

futura convenção para aprofundar as linhas comuns no direito interno. Observa-se que as legislações citadas da Suécia, da República

Federal da Alemanha e da França guardaram certa conformidade com esta resolução, notadamente, quando trata da qualificação da informação, como dado sensível e do direito do titular dos dados de ter conhecimento sobre a coleta de seus dados pessoais (BUTARELLI, 1997, p. 04).

Embora alguns países, a exemplo de Portugal e Espanha tenham tratado sobre a proteção dos dados pessoais em suas respectivas constituições, observou-se que a disciplina da matéria apenas pelo direito interno de cada país membro da U. E ainda não seria suficiente. A coleta e o tratamento de informações pessoais poderiam ser feitos fora dos limites de um Estado, surgindo assim, a necessidade de uniformizar a legislação em matéria de proteção de dados.

Desde 1960, a Organização para Cooperação e Desenvolvimento Econômico – OCDE tem a preocupação de instituir um regime de proteção dos sistemas informatizados de dados, com enfoque inicial para suas repercussões favoráveis no âmbito da prestação de serviços e no seu poder alavancador da produtividade e resultados econômicos. Assim, foi criado um grupo sobre a utilização de computadores, com o objetivo de analisar os impactos da informática e telecomunicações no desenvolvimento econômico (SAMPAIO, 1998, p. 504).

Dessa forma, a OCDE passou a se preocupar mais com o tema, produzindo um simpósio denominado "Fluxo Transfronteira de Dados e a Proteção da Intimidade", com a participação de um grupo de estudiosos em tráfego transfronteiriço de dados, com o objetivo de elaborar um modelo de lei para o tráfego internacional de dados.

Deste trabalho, resultou o documento intitulado *Guidelines on the protection of privacy and Transborder Flows of Personal data,* que traçava princípios para a disciplina da proteção de dados.

A preocupação central seria o tráfego de dados e não a tutela da pessoa em face de sua utilização.

A sorte deste documento, segundo Doneda (2006, p. 231) foi a de se tornar uma referência comum na área. No entanto, as suas prescrições não chegaram a ser vinculantes, pois os países membros não eram obrigados a legislar conforme as *Guidelines,* tampouco essas tinham influência no seu direito interno.

O enfraquecimento das *Guidelines* fez com que o Conselho da Europa pretendesse regular a matéria de forma integrada, com a elaboração da Convenção 108/1981, para proteção dos Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais.

Esse documento foi conhecido como Convenção de Strasbourg e tinha a pretensão de incitar os Estados-membros a adotar normas específicas para o tratamento de dados pessoais. Este regramento teve um perfil universalista, já que não foi estruturado como uma convenção europeia, tendo sido aberta a países não membros do Conselho de Europa.

A Convenção de Strasbourg foi considerada o ponto de partida do modelo europeu de proteção de dados pessoais. Seu objetivo era garantir a toda pessoa, de qualquer nacionalidade, o respeito aos direitos e liberdades fundamentais, especialmente o direito à privacidade em face do tratamento automatizado de dados de caráter pessoal. A despeito de voltar-se à proteção das liberdades fundamentais, notadamente da privacidade, o Preâmbulo desse documento reafirma o seu empenho em favor da liberdade de informação sem limite de fronteiras[7].

[7] O Preâmbulo da Convenção 108/1981 dispõe que: "Os Estados membros do Conselho da Europa, signatários da presente Convenção: Considerando que a finalidade do Conselho da Europa é conseguir uma união mais estreita entre os seus membros, nomeadamente no respeito pela supremacia do direito, bem como dos direitos do homem e das liberdades fundamentais; Considerando desejável alargar a proteção dos direitos e das liberdades fundamentais de todas as pessoas, nomeadamente o direito ao respeito pela vida privada, tem em consideração o fluxo crescente, através das fronteiras, de dados de carácter pessoal susceptíveis de tratamento automatizado; Reafirmando ao mesmo tempo o seu empenhamento a favor da liberdade de informação sem limite de fronteiras; Reconhecendo a necessidade de conciliar os valores fundamentais do respeito à vida privada e da livre circulação de informação entre

Após o advento dessa Convenção, vários países passaram a legislar acerca desta matéria, alguns inclusive, legislando pela primeira vez. A Bélgica aprovou em 1992 uma lei de proteção da vida privada com respeito ao tratamento de informações pessoais. Atendendo à disposição da Constituição de 1978, a referida lei voltou-se a limitar o uso da informática para garantir a honra e a intimidade pessoal e familiar que começou a vigorar na Espanha.

O direito à privacidade encontrou algumas resistências no direito britânico. Malgrado o Reino Unido ter aderido à Convenção de Strasbourg, promulgando a *Data Protection Act, em 1984,* a matéria foi tratada de forma peculiar no país, não se reconhecendo a existência de um direito à privacidade. Naquela legislação, tutelava-se a pessoa apenas contra intromissão não autorizada na sua vida privada, pelo uso abusivo de informações pessoais (DONEDA, 2006, p. 233).

Não obstante a Convenção de Strasbourg ter sido considerada como ponto de partida do modelo europeu de proteção de dados pessoais, somente em 1995 surgiu um documento que conseguiu padronizar de forma efetiva a proteção de dados pessoais na União Europeia: a Diretiva 95/46/CE, do Parlamento Europeu e Conselho da Europa. Em virtude de sua importância, este documento, será analisado em tópico individual.

3.2.1.1 Os principais aspectos da Diretiva 95/46/CE

A Diretiva 95/46/CE foi um documento de grande importância para a história da proteção de dados pessoais, não só nos países integrantes da União Europeia, como também em outros países que se utilizaram deste modelo para criar as suas legislações nacionais sobre o tema.

---

os povos, acordam o seguinte: {...}". (CONVENÇÃO 108/1981. Disponível em: http://www.cnpd.pt/bin/legis/internacional/concenca0108.htm. Acesso em: 01 de jul. 2014).

Essa normativa teve a função precípua de uniformizar a legislação sobre proteção de dados pessoais na União Europeia. Apesar da Convenção de Strasbourg ter sido considerada referência na matéria, não foi tão ousada quanto a Diretiva 95, que estabeleceu para os Estados-membros, a obrigatoriedade de criar normas de proteção de dados pessoais, em respeito às suas orientações gerais.

O objetivo desta Diretiva foi assegurar a proteção das liberdades e dos direitos fundamentais das pessoas singulares, especialmente o direito à vida privada em face do tratamento de dados pessoais. Considerando o fluxo internacional dos dados[8], o documento pretendia a uniformização do seu tratamento pelos países integrantes da U.E, visando evitar legislações contraditórias.

Por outro lado, a Diretiva 95/46/CE estabelecia como fim primordial à proteção da pessoa em relação ao tratamento de dados pessoais; por outro, tinha a missão de fomentar o comércio por meio de regras comuns para proteção de dados na região, como exigência de um mercado unificado como o europeu. Como se observa nas suas considerações de número 03:

> Considerando que o estabelecimento e o funcionamento do mercado interno no qual, nos termos do artigo 7º A do Tratado, é assegurada a livre circulação das mercadorias, das pessoas, dos serviços e dos capitais, exigem não só que os dados pessoais possam circular livremente de um Estado-membro para outro, mas igualmente, que sejam protegidos os direitos fundamentais da pessoa (DIRETIVA 95/46/CE. Disponível em: http://www.ec.europa.eu, Acesso em: 30 de jun. 2014).

[8] Logo o art. 1º da Directiva 95/46/CE traz o objetivo de tal documento: "1. Os Estados-membros, assegurarão, em conformidade com a presente Directiva, a proteção das liberdades e dos direitos fundamentais da pessoa singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais. 2. Os Estados-membros não podem restringir ou proibir a livre circulação de dados pessoais entre Estados-membros por razões relativas à proteção assegurada por força do nº1. Disponível em: http://www.ec.europa.eu. Acesso em: 01 de jul. 2014.

Nesse sentido, Doneda (2006, p. 237) identifica dois eixos em torno da disciplina de proteção de dados pessoais: o primeiro seria a proteção da pessoa e a necessidade de proporcionar a livre circulação de pessoas, mercadorias, serviços e capitais, implicando a utilização de dados pessoais e o segundo eixo seria a presença de um critério de equilíbrio entre ambos, que é a referência ao homem e aos seus direitos fundamentais.

Tanto essa Diretiva quanto as legislações que surgiram posteriormente, foram baseadas em princípios gerais de tutela, que são variáveis de lei para lei, de doutrina para doutrina. Para os fins deste estudo, adotar-se-ão, com prioridade, os princípios previstos na Diretiva que serviu de modelo para elaboração da maior parte das legislações sobre proteção de dados pessoais. Portugal, Itália, França, Áustria, Grécia, Alemanha, Irlanda, Luxemburgo, Suíça e Inglaterra são países nos quais existe legislação sobre proteção de dados pessoais.

Muito embora estes princípios constem na maior parte das Diretivas do Parlamento Europeu e do Conselho da Europa, relacionadas à privacidade, nem todas as legislações nacionais dos países integrantes da U.E os previram expressamente. Isto, contudo, não impede a sua aplicação pela jurisprudência, na medida em que são considerados como base do sistema de proteção de dados pessoais.

Dentre os princípios mais importantes, citam-se: o princípio da transparência; o princípio da lealdade ou da boa-fé; o princípio da publicidade; o princípio da proporcionalidade; o princípio da veracidade dos dados; o princípio da caducidade; o princípio da segurança no tratamento dos dados; o princípio da confidencialidade; o princípio do não tratamento dos dados sensíveis; o princípio da reciprocidade das vantagens e o princípio da responsabilidade objetiva.

Pelo princípio da transparência ou da publicidade, todo o sistema de coleta e tratamento de dados deve ser do conhecimento público. Todas as pessoas cujos dados hajam sido coletados,

registrados, tratados ou armazenados em bancos devem ter ciência do tipo de informação envolvida, bem como a finalidade da operação. O referido princípio pode ser visto em diversas legislações, como por exemplo, na Lei sueca de 1973, bem como na Lei francesa de 1978.

Na Diretiva 95/46/CE, no seu artigo 10, pode-se encontrar menção ao princípio da publicidade ou transparência:

> Os Estados-membros estabelecerão que o responsável pelo tratamento ou o seu representante deve fornecer à pessoa em causa junto da qual recolha dados que lhe digam respeito, pelo menos as seguintes informações, salvo se a pessoa já delas tiver conhecimento:
> a) Identidade do responsável pelo tratamento e, eventualmente, do seu representante;
> b) Finalidades do tratamento a que os dados se destinam; {...}. (DIRETIVA 95/46/CE. Disponível em: http://www.ec.europa.eu, Acesso em: 30 de jun. 2014).

O princípio da transparência impõe que a pessoa seja informada de forma detalhada sobre o tratamento de dados a seu respeito, como identificação do responsável pelo banco de dados, a finalidade do tratamento e outras informações que possam ser relevantes para o seu titular. Requer o consentimento expresso do indivíduo, podendo ser dispensado, nos casos em que os dados são obtidos e coletados pelo próprio poder público,

O princípio da lealdade ou da boa fé estabelece que todo tipo de tratamento de dados pessoais deve ser levado a efeito, levando-se em consideração a realização dos objetivos propostos, assim como a autorização do titular para a finalidade almejada. Dessa forma, pode haver violação ao princípio da boa fé ou da lealdade, na coleta de dados sem a autorização do seu titular, bem como a criação de um banco de dados para traçar perfil das pessoas e posterior comercialização com empresas.

Verifica-se que a única hipótese que pode ser identificada para utilização de dados pessoais com finalidade diversa da qual foi

concedida, é aquela quando os dados são coletados pelo Estado para preservar interesse público, como no caso dos serviços de inteligência da polícia.

Outra questão que se relaciona intrinsicamente ao princípio da boa fé ou da lealdade é o tempo de conservação das informações. O responsável por um banco de dados deverá eliminar todas as informações constantes que ultrapassem determinado tempo. No exemplo da Lei francesa, o art. 28 dispõe que a duração máxima para manutenção de informações pessoais em bancos de dados privados deve ser aquela que constar na própria declaração.

Identifica-se ainda, como princípio de proteção de dados pessoais, o princípio da proporcionalidade que estabelece que os dados pessoais deverão ser adequados, pertinentes e não excessivos relativamente às finalidades para os quais estão sendo recolhidos (DIRECTIVA 95/46/CE, art. 6º, a). Este princípio impõe um juízo de adequação do dado utilizado no tratamento e o fim almejado para a coleta, evitando-se que o indivíduo seja obrigado a conceder informações desproporcionais aos fins a que se destinam. Assegura-se ainda, o direito de se opor à coleta e a tratamento de informações, conforme preceitua o art. 14 da Diretiva 95/46/CE:

> Direito de oposição da pessoa em causa
> Os Estados-membros reconhecerão à pessoa em causa o direito de:
> a) Pelo menos nos casos referidos nas alíneas e) e f) do artigo 7º, se opor em qualquer altura, por razões preponderantes e legítimas relacionadas com a sua situação particular, a que os dados que lhe digam respeito sejam objecto de tratamento, salvo disposição em contrário do direito nacional. Em caso de oposição justificada, o tratamento efectuado pelo responsável deixa de poder incidir sobre esses dados;
> b) Se opor, a seu pedido e gratuitamente, ao tratamento dos dados pessoais que lhe digam respeito previsto pelo responsável pelo tratamento para efeitos de mala directa; ou ser informada antes de os dados pessoais serem comunicados pela primeira vez a terceiros para fins de mala directa ou

> utilizados por conta de terceiros, e de lhe ser expressamente facultado o direito de se opor, sem despesas, a tais comunicações ou utilizações (DIRETIVA 95/46/CE. Disponível em: http://www.ec.europa.eu, Acesso em: 30 de jun. 2014).

Percebe-se a preocupação constante do legislador com o assentimento do titular dos dados, mais especificamente com a vontade do indivíduo de desejar ou não que seus dados sejam transmitidos.

Dessa forma, resta assegurado o direito da pessoa se opor ao tratamento de dados pessoais, quando verificado no caso concreto motivos que justifiquem tal desejo. Assim, deverão ser sopesados tanto os interesses do titular dos dados, como também daquele que solicita informações de determinada pessoa, consubstanciando, assim, o princípio da proporcionalidade. Esse direito de oposição só não poderá prevalecer quando se tratar de imposição legal, como por exemplo, quando o poder público solicita dados pessoais para preservação do interesse público.

Pelo princípio da veracidade ou da exatidão, os dados constantes em bancos de dados devem ser fieis à realidade, de sorte que a coleta e o tratamento destes dados devem ser realizados com o máximo de cuidado e correção para evitar danos à privacidade do titular dos dados.

A Diretiva 95/46/CE, no seu art. 6°, alínea "d", do ítem I, estabelece que os dados pessoais deverão ser exatos e, se necessário, atualizados, devendo-se tomar todas as medidas para assegurar que dados inexatos sejam apagados ou retificados, considerando-se a finalidade para o qual forem recolhidos.

Para que o titular dos dados pessoais possa corrigir aqueles dados inexatos ou incompletos é necessário que se lhe permita o acesso aos respectivos dados, para que, tomando conhecimento, possa decidir pela eventual retificação ou complementação.

A falta de correção ou atualização de dados pessoais inexatos ou incompletos pode causar sérios prejuízos ao seu titular (CASTRO, 2005, p. 237), obrigando os responsáveis pelos bancos

de dados a atualizar estas informações sempre que as correções se fizerem necessárias. Lembre-se que a pessoa que tem em seu poder um banco de dados poderá ser responsabilizada civilmente por armazenar dados inexatos ou incompletos.

Em virtude do princípio da caducidade, as informações constantes destes bancos de dados serão armazenadas somente pelo período considerado necessário para a persecução das finalidades para as quais foram coletados, conforme previsão na Diretiva 95/46/CE, art. 6°, alínea "e"[9] e na Diretiva 2002/58/CE, ítem 23, do preâmbulo.

Por meio desse princípio, os dados que atingirem as suas finalidades, deverão ser apagados, como forma de preservar a intimidade e privacidade dos seus titulares. Na prática, porém, essa exigência parece passar despercebida, principalmente nos contratos celebrados com organizações privadas. Muitas vezes, alcançados os fins para os quais os dados foram coletados, os seus detentores acabam por transmiti-los a outras empresas, sem a autorização ou mesmo o conhecimento do respectivo titular.

Somente excepcionalmente, pode-se admitir que as informações armazenadas permaneçam guardadas por tempo indeterminado, como quando o detentor de tais dados é o Estado, nos casos de dados relacionados à identificação civil da pessoa.

Trata-se do direito ao esquecimento, decorrência do princípio da caducidade, conforme ensina Castro (2005, p. 239-240). Cabe ao individuo exigir que os seus dados pessoais sejam apagados, após o alcance das finalidades para as quais foram recolhidos.

---

[9] Art. 6°. "1. Os Estados-membros devem estabelecer que os dados pessoais serão: (...) e) conservados de forma a permitir a identificação das pessoas em causa apenas durante o período necessário para a prossecução das finalidades para que foram recolhidos ou para que são tratados posteriormente. Os Estados-membros estabelecerão garantias apropriadas para os dados pessoais conservados durante períodos mais longos do que o referido, para fins históricos, estatístico ou científicos". (DIRECTIVA 9546/CE. Publicada no Jornal Oficial n° 281, de 23/11/1995. Disponível em: http://www.eur-lex.europa.eu. Acesso em: 03 de jul. 2014).

Os bancos de dados, públicos ou privados, devem garantir aos titulares de informações pessoais, que seus dados serão protegidos contra os riscos de extravio, destruição, modificação e transmissão ou acesso não autorizado, com fundamento no princípio da segurança no tratamento dos dados pessoais.

A Diretiva 95/46/CE, no art. 17 estabelece que os responsáveis pelo tratamento de dados pessoais devem adotar medidas técnicas e organizativas para proteger os dados pessoais contra destruição acidental ou ilícita, bem como a alteração, difusão ou acesso não autorizado. Tais medidas devem atender aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação, com um nível de segurança adequado em relação aos riscos que o tratamento pode apresentar.

Nesse sentido, o responsável pelo tratamento de dados pessoais deve adotar medidas técnicas e administrativas para garantir a segurança no armazenamento destas informações, evitando-se assim, o acesso não autorizado e a alteração ou a destruição destes dados. Dessa forma, garante-se ao titular o seu direito à intimidade e à privacidade.

O princípio da confidencialidade se apresenta como corolário do princípio da segurança no tratamento, garantindo ao titular dos dados pessoais o sigilo no tratamento destas informações. Ressalta-se que a transmissão destes dados a terceiros, sem autorização do seu titular viola o dever de sigilo, bem como os princípios da lealdade e boa-fé. A transmissão destas informações só se revela como legítima, se for necessária à preservação de outros valores constitucionais.

Este princípio encontra assento no art. 16 da Diretiva 95/46/CE, que estabelece:

> Qualquer pessoa que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratante, bem como o próprio subcontratante, tenha acesso a dados pessoais, não procederá ao seu tratamento sem instruções do responsável pelo tratamento, salvo por foça de obrigações legais (DIRETIVA 95/46/CE.

> Disponível em: http://www.ec.europa.eu, Acesso em: 30 de jun. 2014).

Resta demonstrada a responsabilidade da autoridade pelo tratamento de dados pessoais, até mesmo quando outra pessoa estiver agindo em seu nome, como preposto. É vedado o tratamento dessas informações sem as devidas instruções do responsável pelo tratamento de dados.

À título comparativo, no Brasil, a Lei 12.527/2011, que dispõe sobre os procedimentos a ser observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações, previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal, trata do sigilo das informações estabelecendo que

> Art. 25. É dever do Estado controlar o acesso e a divulgação de informações sigilosas produzidas por seus órgãos e entidades, assegurando a sua proteção.
> § 1º O acesso, a divulgação e o tratamento de informação classificada como sigilosa ficarão restritos a pessoas que tenham necessidade de conhecê-la e que sejam devidamente credenciadas na forma do regulamento, sem prejuízo das atribuições dos agentes públicos autorizados por lei.
> § 2º O acesso à informação classificada como sigilosa cria a obrigação para aquele que a obteve de resguardar o sigilo.
> § 3º Regulamento disporá sobre procedimentos e medidas a serem adotados para o tratamento de informação sigilosa, de modo a protegê-la contra perda, alteração indevida, acesso, transmissão e divulgação não autorizados. (BRASIL, 1988)

Observa-se que a lei mencionada acima trata apenas de dados sigilosos que estiverem em poder dos entes federativos, portanto, não se considera objeto desta lei, as informações constantes em bancos de dados privados. Tal constatação faz com que se revele ainda mais necessária a edição de lei de proteção de dados pessoais no Brasil, tendo em vista os riscos sofridos pela ausência de proteção legal, não só dos dados sigilosos, mas

também de todas as informações que digam respeito aos seus titulares, igualmente merecedoras de tutela por parte do Estado.

No tratamento de dados pessoais, encontram-se informações que revelam características próprias e íntimas do indivíduo, como origem racial, opiniões políticas, convicções religiosas ou filosóficas, bem como dados referentes à saúde e orientação sexual, são os chamados dados sensíveis. Os dados sensíveis, como já mencionado, são aqueles que se referem à intimidade ou esfera privada do indivíduo. Via de regra, só podem ser submetidos a tratamento, mediante autorização do respectivo titular, haja vista o princípio do não tratamento de dados sensíveis (art. 8° da Diretiva 95/46/CE)[10]. Excepcionalmente, esses dados podem ser tratados, sem autorização do seu titular, como no exemplo em que determina o interesse público. Mesmo nestes casos, devem-se adotar medidas de segurança para que sejam asseguradas a integridade e a autenticidade das informações, bem como a preservação do necessário sigilo.

Os meios utilizados para coleta e tratamento de dados pessoais, também podem ser manuseados para o exercício dos direitos conferidos ao seu titular. Se a coleta se faz por meio da internet, o direito do titular acessar as informações a seu respeito, bem como o direito de oposição deverão ser exercidos também pela internet, conforme determina o princípio da reciprocidade das vantagens.

Na prática, verifica-se que este princípio não tem sido eficaz, porque na maioria das vezes os titulares de dados têm dificuldades para acessar informações a eles pertinentes, prejudicando-lhes o controle.

Por último, vale citar o princípio da responsabilidade objetiva dos responsáveis pelo controle das bases de dados pelos

[10] Art. 8° - Tratamento de certas categorias especificas de dados. "1. Os Estados-membros proibirão o tratamento de dados pessoais que revelem a origem racial e étnica, as opiniões politicas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual". Disponível em: http://www.eur-lex.europa.eu. Acesso em: 01 de jul. 2014.

danos causados por conta do descumprimento dos princípios de proteção de dados pessoais citados anteriormente. Nessas hipóteses, a responsabilidade é objetiva, independente de agirem com dolo ou culpa, considerando que se trata de atividade de risco, implicando o dever de indenizar quando cause danos morais ou materiais ao titular dos dados[11].

A grande questão que se coloca na responsabilização objetiva dos danos causados ao titular de dados, é saber quem responsabilizar, tendo vista que muitas vezes torna-se difícil identificar a pessoa responsável, por envolver vários agentes no processo de coleta e tratamento de dados. Por esta razão, necessário se faz a figura do guardião ou responsável pelo tratamento de dados, assim como também revela-se importante identificar a atividade como de risco, implicando a responsabilização objetiva (CACHAPUZ, 2006, p. 278-279).

No entanto, o princípio da responsabilidade objetiva não encontra assento em todas as legislações que tratam da proteção de dados pessoais. Algumas normatizações sobre o tema preferem tratar a responsabilidade como subjetiva, não identificando no caso uma atividade de risco. O Marco Civil da Internet no Brasil – Lei nº 12.965, de 23 de abril de 2014[12], por exemplo, estabelece no art. 18, que o provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros.

A Diretiva 95/46/CE impôs a obrigação aos Estados-membros de editar normas, conforme o conteúdo normativo deste documento e, em 1997 todos os países integrantes da União

[11] O mencionado princípio está previsto no art.23 da Diretiva 95/46/CE, estabelecendo que: "Responsabilidade. 1. Os Estados-membros estabelecerão que qualquer pessoa que tiver sofrido um prejuízo devido ao tratamento ilícito de dados ou qualquer outro acto incompatível com as disposições nacionais de execução da presente directiva tem o direito de obter do responsável pelo tratamento a reparação pelo prejuízo sofrido. 2. O responsável pelo tratamento poderá ser parcial ou totalmente exonerado desta responsabilidade se provar que o facto que causou o dano lhe não é imputável. (UNIÃO EUROPEIA. Directiva 95/46/CE. Op. cit)

[12] Disponível: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/lei/12965.htm Aceso em: 30 de jun. 2014.

Europeia já haviam incorporado o conteúdo de tal documento às legislações nacionais.

Em 15 de dezembro de 1997 foi promulgada a Diretiva 97/66/CE[13], do Parlamento e do Conselho Europeu, com o objetivo de proteção ao tratamento de dados pessoais e à privacidade no setor das telecomunicações. Este documento transpôs os princípios previstos na Directiva 95/46/CE em regras específicas para o setor das telecomunicações.

A Directiva 97/66/CE pretendeu se adaptar ao desenvolvimento dos mercados e das tecnologias dos serviços de comunicações eletrônicas, com o objetivo de proporcionar um nível idêntico de proteção de dados pessoais e da privacidade. No art. 3°, 1, estabelece a sua aplicação ao tratamento de dados pessoais em relação com a prestação de serviços públicos de telecomunicações na Comunidade e, especialmente, através da rede digital de serviços integrados e das redes móveis digitais públicas.

Não obstante a importância que teve a Diretiva 95/46/CE para a proteção de dados pessoais não só nos países integrantes da União Europeia, como também em outros países, em 2002 foi editada a Diretiva/2002/58/CE, de 12 de julho de 2002, do Parlamento e do Conselho Europeu, revogando a normativa 97/66/CE. A Diretiva 2002/58 permitiu a adequação de suas finalidades à evolução tecnológica na área da comunicação em rede, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas.

Na sua consideração de número 11, a Diretiva 2002/58/CE deixa registrado que não trata de questões relativas à proteção dos direitos e liberdades fundamentais relacionados com atividades não

[13] O seu art. 1° dispõe que: "La presente Directiva estabelece la arminización de las disposiciones de los Estados membros para garantizar um nível equivalente de protección de las libertades y de los derechos fundamentales y, em particular, del derecho a la intimidad, em lo que respecta al tratamento de los datos personales em el sector de las telecomunicacionrs, así como a libre circulación de tales datos y de los equipos u servicios de telecomunicación em la comunidade". UNIÃO EUROPÉIA. Directiva 97/66/Ce do Parlamento Europeu e do Conselho de Estado. Disponível em: http://www.http://www.eurlex.europa.eu. Acesso em: 01 de jul.2014.

reguladas pelo direito comunitário. No entanto, não altera o equilíbrio existente entre o direito dos indivíduos à privacidade e à possibilidade dos Estados-membros tomarem medidas necessárias para a proteção da segurança pública, da defesa e da segurança do Estado. Assim, não afeta a capacidade dos Estados-membros, por exemplo, de interceptarem legalmente comunicações eletrônicas, se necessário para atingir os obejtivos expressos para tal documento[14].

Na verdade, a Diretiva 2002/58/CE serviu para especificar e complementar a Diretiva 95/46/CE, não sendo aplicável a atividades fora do âmbito do Tratado que instituiu a Comunidade Europeia, além disso, as suas disposições trataram de assegurar regras de proteção dos legítimos interesses dos assinantes, que são pessoas coletivas.

Ainda no que se refere à Diretiva 95/46/CE, percebe-se a preocupação do Parlamento e do Conselho Europeu em criar uma autoridade ou garante responsável para fiscalização da aplicação no seu território das disposições adotadas pelos Estados-membros, estabelecendo as seguintes regras no seu art. 28:

> 2. Cada Estado-membro estabelecerá que as autoridades de controle serão consultadas quando da elaboração de medidas regulamentares ou administrativas relativas à proteção dos direitos e liberdades das pessoas no que diz respeito ao tratamento de dados pessoais.
> 3. Cada autoridade do controle disporá, nomeadamente:
> - de poderes de inquério, tais como o poder de aceder aos dados objeto de tratamento e de recolher todas as informações necessárias ao desempenho das suas funções de controle.
> - de poderes efetivos de intervenção, tais como, por exemplo, o de emitir parecer previamente à execução adequada desses preceres, o de ordenar o bloqueio, o apagamento ou a

[14] Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002 – relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas. Publicada no Jornal Oficial das Comunidades Europeias, em 31/07/2002. Disponível em: http://www.eur-lex.europa.eu. Acesso em 03 de jul. 2014.

> destruição dos dados, o de proibir temporária ou definitivamente o tratamento, o de dirigir uma advertência ou uma censura ao responsável pelo tratamento ou o de remeter a questão para os parlamentares nacionais ou para outras instituições políticas. {...} (DIRETIVA 95/46/CE. Disponível em: http://www.ec.europa.eu, Acesso em: 30 de jun. 2014).

Verifica-se que a autoridade garante tem como objetivo fiscalizar e controlar o tratamento de dados pessoais, devendo exercer funções consultivas, administrativas, de investigação, de representação internacional e esclarecimentos, devendo-se garantir a independência e a imparcialidade no exercício de tais funções. Este órgão faria as vezes de uma agência reguladora, como as que existem aqui no Brasil, como por exemplo, a Agência Nacional de Telecomunicações – ANATEl.

Além da autoridade fiscalizadora e de controle no tratamento de dados pessoais, há previsão no art. 29 e 30 da Diretiva 95/46/CE para criação de um grupo de proteção das pessoas no que se refere ao tema. Este grupo seria criado por um representante da autoridade de controle designada por cada Estado-membro, por um representante da autoridade ou autoridades criadas para as instituições e organismos comunitários, bem como por um representante da Comissão.

Cada membro seria designado pela instituição ou autoridades que representa com as seguintes atribuições, conforme o art. 30 da Diretiva 95/46/CE: a) analisar quaisquer questões relativas à aplicação das disposições nacionais tomadas nos termos da Directiva 95; b) dar parecer à Comissão sobre o nível de proteção na Comunidade e nos países terceiros; c) aconselhar a Comissão sobre quaisquer alterações da Diretiva ou sobre quaisquer medidas adicionais para proteger direitos e liberdades no que diz respeito a dados pessoais e; d) dar parecer sobre os códigos de conduta elaborados em nível comunitário.

Vale destacar que, muito embora, a Directiva 95/46 tenha sido considerada um dos documentos mais importantes da União

Europeia acerca da proteção de dados pessoais, entrou em vigor em maio de 2018, o novo Regulamento de proteção de dados pessoais. Trata-se do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho e, por ser um "regulamento", não carece de transposição para a lei dos Estados-Membros, conforme ocorre com as "diretivas".

3.2.1.2 O modelo italiano de proteção de dados pessoais

A Itália, ao contrário de outros países europeus, somente legislou sobre proteção de dados pessoais quando se ultimava o prazo estabelecido pela Diretiva 95/46/CE. Tal documento concedia aos Estados-membros o prazo de até três anos para que houvesse a transposição da Directiva às legislações nacionais.

Observa-se que a matéria atinente ao direito à privacidade foi ignorada pela doutrina italiana por muito tempo. O Código Civil de 1865 praticamente não tratou do tema e o *diritto alla riservatezza* somente foi considerado quando da reforma do referido código.

Já o Código Civil italiano de 1942 previa expressamente a proteção à privacidade no art. 10[15], quando tratou do direito à imagem, da exposição ou publicação abusiva da imagem alheia. No entanto, não mencionava àquela época a privacidade informacional, relativa à proteção de dados pessoais.

Doneda (2006, p. 242-243) lembra que de fato a primeira referência concreta do direito italiano acerca desta matéria se deu com a Convenção Européia para a proteção dos Direitos do Homem e das Liberdades Fundamentais de 1950[16][49], que previa no

[15] O Código Civil italiano de 1942 estabelece no seu art. 10 que: "Qualora l'mmagine di una persona o dei genitori, del coniuge o dei figli sai stata esposta o pubblicata fuori dei casi in cui l'esposizione o la pubblicazione e dalla legge consentita, ovvero com pregiudizio al decoro o ala reputazione della persona stessa o dei detti congiunti, l'autorità giudiziaria, su richiesta dell'interessato, può disporre che cessi l'abuso, salvo il risarcimento dei danni". (Disponível em: http://www.ligiera.com.br. Acesso em: 30 de jun. 2014).

[16] A Convenção Europeia dos Direitos Humanos foi adotada pelo Conselho da Europa em novembro de 1959 e, entrou em vigor em 1953. Esta Convenção instituiu o Tribunal Europeu dos Direitos Humanos e o Comitê de Ministros do Conselho da Europa. O art. 8° da referida convenção dispõe que: "1. Qualquer pessoa tem direito ao respeito à vida privada e familiar, do seu domicilio e da sua

art. 8º o respeito à vida privada e familiar. Assim, a proteção da pessoa passou a ser analisada em um novo contexto, inclusive pela jurisprudência italiana que também passou a reconhecer um *diritto alla riservatezza*.

Em um caso julgado pelos tribunais italianos, chamado de "caso Petacci", a Corte de Apelação de Milão considerou que a publicação de fato da vida privada de uma pessoa seria uma violação do *diritto alla riservatezza,* considerado reflexo do direito geral de personalidade e não um direito autónomo, em semelhança do que entendera a Corte Alemã. No caso, a família de Clara Petacci solicitava a retirada de circulação de uma novela, intitulada "O grande amor", que veiculava suposta relação amorosa entre ela e Mussolini (DONEDA, 2006, p. 244).

Foi somente na decada de 1970 que as cortes italianas começaram a reconher a existência de um *diritto alla riservatezza,* como situação jurídica autônoma. A preferência por tal expressão, a doutrina italiana passou a utilizar o termo *privacy*, denotando a influência pelo *right to privacy,* de Warren e Brendeis.

Mas o *diritto alla riservatezza* e a *privacy* não se confundem no direito italiano (DONEDA, 2006, p. 248). O primeiro permanece com uma noção de reserva e isolamento pessoal, construída pela doutrina e assimilada pela jurisprudência. Já a expressão *privacy* corresponde a outra ordem de preocupação, mais relacionada ao tratamento de dados pessoais.

Como o alargamento do termo *diritto alla riservatezza* como uma complexa tutela de informações pessoais não seria possível, elegeu-se o termo *privacy* para representar a nova dimensão da privacidade, pertinente à proteção de dados pessoais.

---

correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito, senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para segurança nacional, para a segurança pública, para o bem-estar econômico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros"(CONVENÇÃO EUROPÉIA DOS DIREITOS DO HOEMEM. Disponível em: http://www.echr.int/documents/convention_POR.pdf. Acesso em: 28/06/2014

A sociedade italiana começou a despertar para questões ligadas à utilização de informações pessoais em alguns episódios ocorridos desde a década de 1950. À título exemplificativo, no ano de 1954, o Conselho de Ministros deliberou uma série de medidas administrativas de cunho discriminatório em relação às pessoas inscritas no Partido Comunista italiano. Posteriormente, em 1964, descobriu-se que o ex-serviço secreto militar mantinha um banco de dados relativos a 150.000 cidadãos, dos quais 731 poderiam ser presos e deportados por causa de suas opiniões e atividades políticas.

Em 1971, a imprensa italiana divulgou que o fabricante de automóveis - FIAT havia utilizado informações provenientes de militares e do serviço secreto que remontavam o serviço à época da ditadura fascista, na seleção de seus empregados, (RODOTÁ, 1973, p. 1920).

A divulgação destes fatos envolvendo o vazamento de informações pessoais culminou com uma maior preocupação da Itália acerca da proteção de dados pessoais. Havia uma pressão para que fosse elaborada uma lei nesta matéria desde a década de 1970, no entanto, somente em 1996, o país resolveu legislar acerca deste assunto. Foi o penúltimo país integrante da União Europeia a editar uma lei específica sobre o tema.

A Lei n. 675, de 31 de dezembro de 1996 foi a primeira na Itália a tutelar as pessoas quanto ao tratamento de informações pessoais, transpondo a Diretiva 95/46/CE da União Europeia. Instituiu um sistema de proteção de dados pessoais nos moldes europeus, fixando um sistema de autorizações e reponsabilidades para quem realiza tratamento de dados pessoais. Todavia, essa lei sofreu várias modificações, algumas das quais, logo após a sua promulgação, justificando as severas críticas que lhes foram dirigidas o que a levou a ser alvo de severas críticas.

Essas alterações podem ser justificadas, em primeiro lugar, pelo fato do legislador italiano fazer a opção de integrar posteriormente algumas lacunas contidas na Lei 675, diante das dificuldades em adaptar os interesses dentro do prazo estabelecido

pela Directiva 95/46/CE; de outro lado, justifica-se também tais modificações, pela própria natureza e complexidade da matéria, no que diz respeito a toda estruturação, seja normativa ou administrativa, requerendo um grau de flexibilidade, que foi favorecido pela possibilidade de posterior edição da Lei n. 676/96 (DONEDA, 2003, p. 06).

A Lei n. 676/96 delegou ao executivo a faculdade de legislar sobre o estabelecimento de parâmetros para posterior integração da lei anterior, o que de fato foram feitas várias modificações nos anos seguintes, por meio de Decretos Presidenciais e Legislativos, formando assim, o núcleo duro da matéria de proteção de dados pessoais na Itália.

Dessa forma, o Parlamento italiano, por meio da Lei Delegada nº 127, estabeleceu em 24 de março de 2001, que o Poder Executivo deveria elaborar um documento único em matéria de proteção de dados pessoais, com o objetivo de coordenar o conjunto de normas vigentes e efetuar as modificações necessárias.

Como resultado, foi publicado o "Codice in matéria di protezione dei dati personali", por meio do Decreto Legislativo nº 196, de 30 de junho de 2003, que entrou em vigor em 1º de janeiro de 2004. A sua base de elaboração foi a proteção de dados pessoais como direito fundamental. A opção pela disciplina por meio de um código já denotaria a intenção de se estabelecerem normas sectoriais sobre a matéria (DONEDA, 2003, p. 07).

O *Codice in materia di protezione dei dati personali* divide-se em três partes:

> disposições gerais; parte especial, denominada de Disposições relativas a setores específicos e; uma última parte denominada Tutela do interessado e sanções. A primeira parte fixa os regramentos a ser aplicados a todas as modalidades de dados pessoais. Na segunda, fixam-se as regras específicas para determinados setores. E, por último, na terceira parte, estabeleceram-se as disposições sobre o sistema e os instrumentos de tutela adotados (DECRETO LEGISLATIVO 196/2003).

Logo no início das Disposições Gerais, percebe-se a preocupação do legislador em consagrar o direito à proteção de dados pessoais como direito fundamental, afastando-se da nomenclatura utilizada pelo direito alemão "direito à autodeterminação informativa" ou de qualquer outra ideia que remetesse a uma associação entre privacidade e o direito de propriedade.

Tal afirmação com ênfase na proteção da pessoa serve para demonstrar que embora tal código realize a transposição da Diretiva 95/46/CE, leva em consideração uma concepção de sociedade da informação, pela qual se faz necessário instrumento jurídico hábil a contrastar uma lógica de livre fluxo de informações pessoais, cabendo ao Estado promover o respeito à pessoa e às suas informações.

O Código em matéria de proteção de dados pessoais compreende, segundo Rodotá (2008, p. 198), a lei instituidora nº 675, de 31/12/1996, os dez decretos legislativos sobre disposições integrativas ou corretivas daquela lei e, muitas outras normas dispersas do sistema. Levou-se em consideração uma lógica que não é só reprodutiva, mas que leva em conta o trabalho realizado em seis anos precedentes pelo Garante para a proteção dos dados pessoais, quando da aplicação da primeira lei italiana sobre a matéria. Dessa forma, Rodotá adverte que:

> Ele representa a primeira tentativa, em escala internacional, de reordenação geral de uma matéria complexa e, sobretudo, extraordinariamente móvel. É estruturado de acordo com módulos diversos, mas possui uma organização na qual possui particular relevância o contexto dos princípios (RODOTÀ, 2008, p. 198).

Nesse sentido, se mostra relevante fazer a distinção entre o tradicional direito à privacidade e a privacidade informacional, como proteção de dados pessoais. No primeiro sentido se manifesta o momento individualista, ligado ao isolamento e ao

recato. Já no que diz respeito à proteção de dados pessoais, fixam-se regras sobre as modalidades de tratamento dos dados, concretizando-se em poderes de intervenção. Tais poderes de intervenção e controle são atribuídos não só aos interessados diretos, mas também a uma autoridade garante, envolvendo assim, uma responsabilidade pública específica.

Aqui se percebe, na opinião de Rodotá (2008, p. 199), o ponto de chegada de uma longa evolução do conceito de *privacy*: da sua originária definição do *direito a ser deixado só* até o direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada.

Essa evolução pode ser também percebida na Carta dos Direitos Fundamentais da União Europeia, quando realiza a distinção entre o direito ao respeito à própria vida privada e familiar (art. 7°) e o direito à proteção de dados pessoais (art. 8°)[17].

Logo no art. 1° do *Codice in materia di protezione dei dati personali,* reproduzido pelo art. 8° da Carta dos Direitos Fundamentais, percebe-se a manifestação da exata axiologia da Carta, que procurou tutelar "novos" direitos da era tecnológica, sem qualificá-los como direitos de última geração, mas sim em um quadro de indivisibilidade de direitos fundamentais.

Relativamente à proteção de dados pessoais, destaca-se o princípio da necessidade, previsto no art. 3° do Código, que estabelece que os sistemas informativos devem reduzir ao mínimo a utilização de dados pessoais e dados identificadores, quando as finalidades perseguidas em cada caso possam ser alcançadas mediante, dados anônimos ou regras específicas que permitam a identificação do interessado somente em caso de necessidade.

---

[17] A Carta dos Direitos Fundamentais da União Europeia de 2010 dispõe que : "Art. 7°. Todas as pessoas têm direito ao respeito à sua vida privada e familiar, pelo seu domicilio e pelas sua comunicações". "Art. 8° - 1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito". 2. Esses dados devem ser objeto de um tratamento leal para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligados que lhes digam respeito e de obter a respectiva rectificação". (Disponível em: http://www.eur-lex.europa.eu. Acesso em 27 de jun. 2014).

Nessa perspectiva, Rodotá (2008, p. 202) contesta a tendência em se utilizar qualquer inovação tecnológica para tratar dados pessoais. Trata-se de um indicativo importante que deve ser confrontado com uma situação concreta na qual a proteção de dados pessoais parece cada vez mais comprimida diante das exigências de segurança e interesses da empresa. A proteção de dados estaria sob o risco contínuo de ser esmagada pela oferta crescente de tecnologias que facilitam as formas generalizadas de coleta e controle de informações.

O Código de proteção de dados pessoais na Itália presta-se a uma leitura pretensamente "unilateral" (DONEDA, 2006, p. 258), considerando que ao se reforçar a estruturação da disciplina em torno da proteção da pessoa e dos direitos fundamentais, poderse-ia argumentar que o referido documento teria se afastado da ideia de uma disciplina integrada dos dados pessoais, que determinasse garantias positivas para seu livre fluxo, como sugere a Diretiva 46/96/CE.

Essa interpretação se deve à ausência de garantias sobre este fluxo, bem como pela emergência do chamado princípio da necessidade, segundo o qual a utilização de dados pessoais deve reduzir-se a um mínimo necessário para a realização da finalidade perseguida.

O fluxo de informações está intimamente relacionado ao desenvolvimento tecnológico, bem como à integração dos mercados internacionais, cabendo ao Direito, um papel regulador capaz de assegurar um nível mínimo de segurança. Dessa forma, o Código de proteção de dados pessoais italiano procurou estabelecer parâmetros para a tutela dos dados pessoais, impondo limites ao seu livre tratamento e circulação.

Percebe-se que o fluxo livre de dados estaria garantido pelo direito à livre atividade de empreendimento, ou até mesmo pelo direito à liberdade de expressão. No entanto, há de se reconhecer a importância da fixação de limites à liberdade do empreendedor, assim como também pelo fato de representar uma plataforma

segura para desenvolver a atividade negocial. Tais limites irão proporcionar ao consumidor o respeito aos seus dados pessoais (DONEDA, 2006, p. 259).

Por fim, há de se ressaltar a importância do *Garante* para a legislação codificada italiana, cuja função impõe a garantia de difusão e o respeito aos códigos de boa conduta (art. 12). Trata-se de órgão colegiado independente que tem a função de comunicar ao Parlamento e ao Governo a oportunidade de intervenções normativas para tutelar os direitos previstos no art. 2°. Este órgão ocupa posição de destaque para decidir que regras apresentam maior incidência sobre os cidadãos na proteção de seus dados pessoais.

Este órgão que representa o *Garante n*a legislação italiana é composto por quatro membros, sendo dois deles eleitos pela Câmara dos Deputados e dois pelo Senado da República. São escolhidos entre pessoas que assegurem independência e que sejam especialistas de notória competência nas matérias do direito e da informática. Verifica-se que a legislação italiana optou por uma composição pretensamente democrática.

3.3 O modelo norte-americano de proteção de dados pessoais

O *right to privacy* surgiu no direito norte-americano, no famoso ensaio de Warren e Brandeis, em 1890, sendo considerado o antecedente de maior relevo para a noção de direito à privacidade. Por esta razão, dedica-se neste trabalho um tópico para se analisar a proteção de dados pessoais no direito daquele país.

No entanto, sabe-se que até o final do século XIX, não se tinha uma proteção à privacidade, principalmente pelos tribunais norte americanos. Até àquela época, as Cortes se ocupavam de situações que envolviam as violações à propriedade privada. Havia certo receio em que uma eventual tutela a bens da esfera íntima pudessem levar a um aumento dos litígios.

A noção original de *privacy* estava relacionada com um ideal de liberdade, particularmente tutelado na América rural, por um modelo de *property rights*. Em um país com características predominantemente rural, os danos causados por intromissão na vida alheia não se mostravam com grande relevância. Naquela época não havia ainda meios de comunicação, como rádio, jornais, televisão e principalmente computador, que só surgiram tempo depois. Assim, a eclosão do direito à privacidade nos EUA se deu com a passagem de um perfil rural para um perfil urbano (DONEDA, 2006, p. 265).

O direito norte-americano tem sede no sistema denominado de *commom law,* cuja principal fonte são os precedentes judiciais.[18] No entanto, a origem do direito à privacidade nos EUA não se deu por intermédio de um caso específico, mas do artigo de Samuel D. Warren e Louis D. Brandeis, em 1890, intitulado de *The right of privacy*. Neste trabalho, ressaltaram a preocupação que o ataque à intimidade e vida privada das pessoas deixasse de ser uma prática de indivíduos ociosos para se tornar um negócio rentável por parte de sectores como a imprensa. Com isso, o ensaio dos autores americanos foi uma fonte importantíssima para a criação doutrinária da *privacy*.

De qualquer sorte, percebe-se que a noção de *privacy* estava vinculada à ideia de isolamento e recato, o direito de ser deixado em paz, como entediam os autores do célebre artigo. No entanto, naquela época não se fazia menção expressa à privacidade informacional, que os alemães chamariam de autodeterminação informativa.

O fato é que a doutrina teve forte influência na formação e desenvolvimento do *right to privacy,* inclusive de maneira mais intensa do que é habitual na *common law*. Nesse sentido, Doneda esclarece que:

[18] Todavia, o triunfo da *commom law* nos Estados Unidos não foi tão fácil, isto porque muitas regras deste sistema nunca chegaram a ser introduzidas nos EUA, porque não se adaptavam ás condições prevalentes na América. (RENÉ DAVID, 2002, p. 454).

> Esse aspecto "formativo" da doutrina, que já se percebe com certeza, assumiu basicamente duas formas: na primeira, tentou-se estabelecer as bases do que seria uma proteção à privacidade baseada em precedentes e demonstrando a existência de uma tutela da privacidade na *case law* norte-americana; na segunda, procurou organizar de uma forma mais ou menos sistemática o *right to privacy,* seja através do seu enraizamento no *common law* ou então vinculando-o à Constituição norteamericana (DONEDA, 2006, p. 267)

Não obstante o importante papel da doutrina na formação e desenvolvimento do *right to privacy,* não se pode olvidar que o direito norte-americano é caracterizado pela força jurisprudencial, no qual a Suprema Corte desempenha papel fundamental na aplicação dos direitos e garantias fundamentais. Atualmente, após mais de um século de aplicação do *right to privacy* pelo direito norte-americano, não deve causar surpresa, segundo Pinto (1993, p. 512), que se tenha comparado a um direito geral de personalidade.

Todavia, revela-se arriscado incluir a totalidade dos direitos fundamentais na noção de *right to privacy,* devendo-se identificar dentre os aspectos deste direito, aquele que se refere à privacidade informacional. A privacidade no direito norte-americano assume diferentes modalidades, nas quais se protegem situações igualmente diversas.

A fragmentação deste direito se deve, em grande medida, ao peculiar processo de sua formação histórica, bem como ao conjunto de fontes normativas que se relacionam ao conceito de privacidade. De fato, observa-se que o direito à privacidade foi se consolidando lentamente pelo trabalho dos tribunais norte-americanos, ainda que sofrendo uma interrupção, com a decisão do caso *Roberson v Rochester Folding Box Co,* em 1902, quando foi negado o *right to privacy,* por maioria de votos, pela ausência de

precedentes e pelo receio no aumento no número de litígios com a finalidade de um eventual direito à privacidade[19].

No entanto, logo depois, em 1905, a Suprema Corte do Estado da Geórgia, reconheceu os pontos de vista de Warren e Brandeis, naquele que foi considerado *leading case* do direito à privacidade – caso *Pavesich v. New England Life Insurance Co* (DONEDA, 2006, p. 274)[20]. Trata-se de precedente em que uma pessoa teve sua foto e seu nome utilizados para fins publicitários, sem sua autorização.

No caso *Pavesich*, a sentença traçou um verdadeiro perfil do *right to privacy* para, ao final, decidir a favor de *Pavesich*. Dentre os argumentos utilizados na decisão, citam-se:

> a) os precedentes do *right to privacy* são encontrados na tutela contra as moléstias ao sossego, decorrentes de ruídos e na proteção à casa; b) os seus fundamentos eram buscados na Constituição dos Estados Unidos e da Geórgia, especialmente quando declaravam "que ninguém será privado de sua liberdade, a não ser através do devido processo legal" (5ª emenda à Constituição Federal); c) os seus limites encontrados em outros direitos, como por exemplo, a liberdade de expressão e de imprensa, ou seja, caso a publicação tivesse interesse público prevalecia estas liberdades e; d) a renúncia, que ocorre quando alguém resolve ocupar função pública, o que de qualquer forma renuncia em parte ao seu direito à privacidade, no entanto, não

[19] O caso *Roberson v Rochester Folding Box Co* foi julgado pela Suprema Corte de Nova Iorque, em 1902, reformando a decisão que concedera indenização a Abigail Roberson (um bebê) pelo fato de sua imagem ter sido publicada em 25.000 cartazes publicitários, bem como em sacos de farinha comercializados pela empresa demandada. Da decisão deste tribunal, identifica-se como voto divergente e vencido, do *justice* Gray, que se filiou aos argumentos de Warren e Brandeis no seu ensaio *Right to privacy,* publicado doze anos antes. (*Roberson v Rochester Folding Box Co,* 171 N.Y.538 (1902). Disponível em: http://faculty.uml.edu;sgallagher/roberson.htm. Acesso em: 23 de may. 2013.

[20] O referido caso trata-se de episódio envolvendo o uso publicitário de imagem fotográfica, não autorizada, de Paolo Pavesich e de acusação de falsa declaração por companhia de seguros. Na decisão, ficou estabelecido que o fato da inexistência de precedentes sobre determinada matéria não implica na inexistência do direito, pois cabe aos tribunais a utilização de princípios jurídicos para a resolução da lide. Disponível em: http://www.faculty.uml.edu/sgallagher/pavesich_v.html. Acesso em: 23 de may. 2013.

> se modo absoluto, pois até mesmo o Presidente da República tem direito a sua vida privada (SAMPAIO, 1998, p. 65).

Posteriormente, a jurisprudência norte-americana ficou oscilando entre negar o direito à privacidade, como fez no caso *Roberson* e reconhecê-lo, como fez no caso *Pavesich,* em 1905, aplicando os argumentos utilizados por Warren e Brandeis. Após a década de 1930 passou a defender de forma veemente o *right to privacy,* com sua menção expressa no *Restatement of Torts.*

Percebe-se a evolução na jurisprudência norte-americana, na medida em que passou a estender a proteção do uso à imagem, independente de ser propaganda comercial ou não. Levou-se em conta tão somente a existência do consentimento do titular da imagem a ser retratada. Como exemplo, o caso *Peed v. Washington Times Co.,* em que se reconheceu o r*ight to be let alone,* diante da publicação pelo Washington Herald da fotografia de uma mulher asfixiada, por inalação de gás na casa de um amigo (SAMPAIO, 1998, p. 66).

A Constituição americana não tratou do *right to privacy*. Ao tempo em que foi escrita (1787), ainda não havia suscitado a preocupação do legislador constituinte, cujo enfoque principal foram as questões relacionadas à separação dos poderes e à organização do Estado. No século XX, a matéria ganhou o destaque constitucional, por intermédio da Suprema Corte do Estado da Geórgia que passou a reconhecer o *right to privacy* no caso *Pavesich (1905).*

O direito norte-americano não reconhece um direito à privacidade perante outros indivíduos, mas tão somente em relação ao Estado. Assim, o *right to privacy* não pode ser aplicado nas relações privadas, muito embora os efeitos de suas decisões possam ser observados nestas relações.

Na verdade, a primeira oportunidade que a Suprema Corte norte-americana expressou sua opinião sobre o novo *right to privacy,* foi no caso *Olmstead v. United States* (DONEDA, 2006, p. 277). Discutia-se acerca da licitude da interceptação de grampos

sem autorização judicial pelo Governo Federal nos telefones de mercadores de bebidas alcoólicas, cujo comércio era ilegal.

Os comerciantes alegavam que a interceptação não era lícita, pois violava a quarta emenda da Constituição americana que protegia as pessoas, as casas, os documentos e outros. No entanto, perante a lei do Estado que originou a interceptação não era considerado um ilícito[21].

Como o Governo Federal fez as interceptações diretamente da central telefônica, local em que tinha livre acesso, não havia como se considerar invasão à propriedade alheia. E a interpretação que se fazia da quarta emenda da Constituição americana era de que tal dispositivo se referia apenas à invasão não autorizada na propriedade alheia, o que caracterizava a *trespass*. Assim, a Suprema Corte norte-americana entendeu que a quarta emenda não se aplicava ao caso.

A decisão da Suprema Corte americana no caso *Olmstead v. United States* suscitou uma série de críticas até os dias de hoje. Os membros da Corte vencidos no citado julgamento escreveram seu próprio *dissent*. À época, Brandeis era juiz da Suprema Corte e sustentou que a interpretação da Constituição deveria levar em conta os progressos da tecnologia, exigindose uma leitura mais atenta da real intenção do legislador, como condição indispensável à modernização da legislação.

De fato, as *dissents* entenderam que a quarta e quinta emendas deveriam ser interpretadas de forma mais ampla como uma proteção da vida privada da intrusão governamental e não apenas como uma questão ligada à propriedade.

A decisão prolatada no caso citado vigorou quarenta anos, até a sua superação pela decisão produzida no caso *Katz v. United*

[21] A quarta emenda da Constituição americana estabelece: "O direito do povo à inviolabilidade de suas pessoas, casas, papéis e haveres contra busca e apreensão arbitrárias não poderá ser infringido; e nenhum mandado será expedido a não ser mediante indícios de culpabilidade confirmados por juramento ou declaração, e particularmente com a descrição do local da busca e a indicação das pessoas ou coisas a serem apreendidas". Disponível em: http://www.mspc.eng.br/temdiv/const_usa01.shtml#eme_4. Acesso em: 30 de jun. 2014.

States (DONEDA, 2006, p. 281), que igualmente discutia a licitude da interceptação telefônica por agentes federais. Por meio desse caso, a comunicação telefônica foi considerada um interesse a ser protegido para a tutela da pessoa, independentemente de questões relacionadas ao espaço geográfico.

Nessa perspectiva, a Suprema Corte americana passou a reconhecer a tese de Brandeis, a partir do caso *Katz v. United States* (1967, 389 U.S. 347,353), contrariando a decisão proferida no caso *Olmstead* e harmonizando-se com a legislação de vários estados, que há tempos já reconhecia que a interceptação telefônica só poderia ocorrer em casos excepcionais.

Conquanto a Suprema Corte haja mudado sua opinião acerca do direito à privacidade com o caso *Katz v. United States*[22], não se pode afirmar que essa decisão firmou um entendimento estável sobre as questões ligadas às novas tecnologias. Dez anos depois, a Suprema Corte não aplicou a mesma regra no caso *Smith v. Mary*land (1979, 442 U.S. 735).

Neste último caso, a Suprema Corte não considerou violação a quarta emenda, o fato de agentes do governo, sem autorização judicial, haverem instalado um aparelho na linha telefônica de um particular com a finalidade de registrar os números discados. Justificou sua decisão na ausência de expectativa de privacidade do usuário em face de eventual solicitação dos dados à companhia telefônica pela polícia ou justiça.

De acordo com Doneda (2006, p. 284), o *right to privacy* previsto na quarta emenda é o que mais se identifica com a proteção de dados pessoais. Aquela natureza de segredo e isolamento que parecia proteger a propriedade foi ampliada, ao longo do tempo, para favorecer a proteção da pessoa e dos seus dados.

---

[22] No caso *Katz v United States,* a Suprema Corte entendeu que houve violação da privacidade em gravação de conversa telefônica, mesmo mantida em cabine pública, considerando que há no caso, expectativa razoável de privacidade por parte do usuário, considerando ilegal a coleta por parte do Estado de informações pessoais obtidas através de conversas telefônicas, sem o conhecimento e consentimento do individuo. Disponível em: http://www.supreme.justia.com/cases/federal/us. Acesso em: 29 de jun. 2014.

Outras modalidades de privacidade podem ser identificadas na Constituição americana, a exemplo da liberdade de expressão prevista na primeira emenda. Todavia, a Suprema Corte procurou balancear a privacidade e a liberdade de expressão, encontrando razões para limitar a expressão.

Na décima quarta emenda da Constituição americana, aprovada em 1868, observa-se a que o legislador não tratou especificamente do direito à privacidade, mas de outras garantias constitucionais, como a liberdade:

> Todas as pessoas nascidas ou naturalizadas nos Estados Unidos e sujeitas a sua jurisdição são cidadãos dos Estados Unidos e do Estado onde tiver residência. Nenhum Estado poderá fazer ou executar leis restringindo os privilégios ou as imunidades dos cidadãos dos Estados Unidos, nem poderá privar qualquer pessoa de sua vida, liberdade ou bens sem o devido processo legal, ou negar a qualquer pessoa sob sua jurisdição igual proteção das leis.

Instituiu a garantia do *due process of law, q*ue foi concebida inicialmente como garantia do processo penal, sendo estendida posteriormente para as áreas civil e administrativa.

Posteriormente à edição desta emenda, a Suprema Corte norte-americana apreciou o famoso caso *Roe v. Wade* (410 U.S. 113, 1973) e reconheceu o r*ight to privacy* de forma ampla na decisão de uma mulher interromper ou não a gravidez. Fundamentou a decisão na décima quarta emenda, vinculando o direito à privacidade à liberdade.

A partir desta decisão, o *right to privacy* assumiu o papel de garantia de várias liberdades, a exemplo daquelas relacionadas à vida familiar, à concepção, à educação etc. Também serviu para fundamentar o direito das pessoas sem laços familiares a ocupar uma mesma habitação (DONEDA, 2006, p. 288).

Registra-se que o caso *Roe v. Wade* foi alvo de críticas por parte da doutrina e jurisprudência, na medida em que os interesses ali debatidos não estavam diretamente relacionados ao tema da

privacidade. Compreendia-se que as questões referentes ao aborto antes de envolverem a privacidade, estavam correlacionadas à autonomia privada ou à liberdade (SUNSTEIN, 1993, p. 68).

Não obstante a importância do papel da Suprema Corte norte-americana na formação do *right to privacy,* a sua posição quanto à tutela da privacidade e divulgação de dados pessoais ainda é bastante tímida. Sequer estabeleceu uma proteção específica á privacidade dos dados pessoais.

A proteção de dados pessoais nos Estados Unidos diverge daquela estruturada na Europa. Muito embora atualmente estejam empenhados em reduzir as diferenças, os modelos americano e europeu adotaram abordagens diferentes sobre o tema, nos últimos anos.

A disciplina do *right to privacy* americana é bastante fragmentada em diversas leis. A primeira delas data de 1903 e corresponde a uma lei do estado de New York que tentou reverter os efeitos da decisão no caso *Robertson, e*m 1902. Após esta primeira disciplina pode-se identificar várias leis estaduais e federais que foram editadas posteriormente, sobre as quais não cabe aqui tecer comentários por não terem sido de grande importância para a formação do direito à privacidade.

Na década de 1970, houve a edição de várias leis federais sobre a privacidade. Mas foram leis pautadas em critérios e campos de atuação diversos. Estabeleciam diferentes tipos de tratamento para os setores público e privado assim como diferentes tipos de remédios adotados e os campos de atuação específicos para cada normativa (DONEDA, 2006, p. 294).

Dentre as normativas editadas nos anos 1970, menciona-se o *Fair Credit Reporting Act (FCRA.* Estabelecia obrigações de segredo e correção para dados financeiros de consumidores tratados por operadores de cadastro de créditos. Posteriormente essa norma veio influenciar inclusive a legislação consumerista brasileira (BENJAMIM, 1997, p. 327).

Em 1974, foi editada a primeira lei norte-americana, o *Federal Privacy Act,* que reconheceu a existência de um direito geral de privacidade, aplicável apenas em relação aos dados dos cidadãos armazenados pelas agências federais[23]. Na *privacy Act* identificam-se alguns avanços no que se refere a dados pessoais. Os cidadãos passaram a ter direito de obter informações acerca de seus dados pessoais, bem como retificá-los na hipótese de haver incorreção, quando estes dados estejam em arquivos governamentais (DONEDA, 2006, p. 296).

Todavia, a normativa que mais se ocupou diretamente do acesso à informação foi a *Freedom of Information Act, e*m 1967, que garantiu o direito de acesso de pessoas e corporações às suas informações constantes em bancos de dados de agências federais. Em 1986, essa norma foi reformada pela *Freedom of Information reform Act,* cuja preocupação maior seria com a segurança pública. Após dez anos de discussões acerca de registros eletrônicos, o Congresso promulgou, em 1996, a *Freedom of Information Act Ammendments,* com o objetivo de atualizar a legislação de acordo com a evolução nas tecnologias de comunicação.

Observa-se que o Congresso americano promulgou uma série de leis sobre privacidade, que limitam o uso de registros médicos, relatórios de crédito e outros dados. Já a União Europeia optou por uma legislação mais ampla, incluindo uma diretriz comum que concede certos direitos fundamentais a seus cidadãos. Como exemplo, o direito de obter cópias de seus registros mantidos por empresas, direito que nos Estados Unidos os cidadãos americanos não possuem.

[23] O *Federal Privacy Act f*oi uma legislação federal que passou a reger no âmbito das agências governamentais federais, as atividades de processamento de dados pessoais armazenados, sendo permitida a divulgação de informações individuais em hipóteses restritas, bem como ampliou o acesso do interessado a seus dados pessoais, inclusive concedendo direito à retificação. Disponível em: http://www.justice.gov/opcl/privstat.html. Acesso em: 23 de may. 2013.

Mesmo assim, as autoridades nos Estados Unidos entendem que a proteção que dispensam aos dados pessoais é igual ou maior que a oferecida na Europa[24].

Os Estados Unidos estão longe de oferecer uma proteção de dados pessoais nos termos que faz a União Europeia. Em 2012, a Comissão Europeia propôs reformas para reforçar os direitos à privacidade *on-line,* o que parecia muito interessante para empresas de tecnologia americana que atuam na Europa. No entanto, representantes das indústrias dos EUA disseram que se importam mais com a internet livre e voltada para os interesses do comércio.

Constata-se, portanto, que os americanos estão mais preocupados com o livre comércio do que com a tutela dos dados pessoais dos cidadãos americanos. Algumas medidas adotadas na Europa são consideradas demasiadamente rígidas por funcionários do governo e entidades de classe nos EUA. Entendem que a abordagem americana, consubstanciada em leis específicas sobre privacidade é mais eficaz do que a legislação ampla europeia, como pretendeu a Diretiva 95/46/CE.

A disciplina do r*ight to privacy* nos Estados Unidos é frágil porque é bastante fragmentada. Talvez por esta razão a proteção dispensada aos dados pessoais naquele país enfrente mais dificuldades operacionais, já que acaba sendo tratado como a privacidade em geral.

Na tentativa de sistematizar a matéria da proteção de dados pessoais, a doutrina passou a reconhecer a existência de uma *Informational privacy.* No entanto, esse reconhecimento só aconteceu no período posterior a *National Data Center*. Na jurisprudência da Suprema Corte, a proteção de dados pessoais não logrou êxito para obter um tratamento específico. Como exemplo, cita-se o caso da *Restatement of Torts,* que negou a responsabilidade nos casos de

[24] Conforme afirmou recentemente Cameron F. Kerry, assessor jurídico do Departamento de Comércio, em entrevista ao *The New York Times,* publicada pela Folha de São Paulo, em 18 de fevereiro de 2013 Disponível em: http://www1.folha.uol.com.br/fsp/newyorktimes/94301-protecao-de-dados-diverge-na-europa-e-noseua.shtml. Acesso em: 01 de jul. 2014.

publicação de dados pessoais, constantes de bancos de dados públicos. (ANDERSON, 1999, p. 153).

Nos dias atuais, percebe-se que uma parte da doutrina norte-americana defende a tese de se adotar princípios mais genéricos para a proteção de dados pessoais, assim como fez a União Europeia. No entanto, observa-se que esta corrente ainda não encontrou eco no direito dos Estados Unidos, pois é forte a concepção de que uma maior transparência nas regras referentes à proteção de dados pessoais permite maior eficiência do mercado e, consequentemente, a confiança do consumidor.

Outra questão que merece destaque em matéria de proteção de dados pessoais é a necessidade de convergência entre os diversos modelos. Não é forçoso reconhecer que as diferentes disciplinas acerca da privacidade informacional nos diversos países fragiliza sobremaneira a tutela deste direito. Quando cada Estado concede tratamento diferenciado nesta matéria, corre-se o risco de não se ter uma tutela efetiva, considerando que hoje o fluxo de informações se dá de forma globalizada.

No entanto, sabe-se que inciativas de leis nessa seara tiveram por objetivo a busca por padrões internacionais comuns para possibilitar o comércio, como por exemplo, as *Guidelines,* citadas anteriormente.

Há uma tendência em se convergir as regras internacionais sobre proteção de dados pessoais com o intuito de evitar contradições e conflitos, estabelecendo-se regras similares em diferentes países. Afinal, em uma sociedade moderna, na qual as informações são facilmente disseminadas, uma efetiva proteção só pode ser percebida se houver um tratamento internacional convergente sobre a matéria.

Todavia, até o ano de 2016, só se podia identificar as normativas de âmbito nacional e, outras de âmbito restrito a blocos de países, como as Diretivas da União Europeia. Não havia normas de âmbito internacional/global, que se destinassem à proteção específica de dados pessoais e que sejam dirigidas a todos os países.

O que fazia com que houvesse uma disparidade de legislações de proteção de dados entre os diversos países, assim como uma consequente redução da sua eficácia.

No âmbito dos países integrantes da União Europeia, várias tentativas foram empreendidas no sentido de harmonizar as diversas regras sobre proteção de dados pessoais, com o fito de facilitar o fluxo internacional de informações, como já foram mencionadas, as *Guidelines e*, posteriormente a Convenção de Strasbourg, em 1981. Entretanto, estas regras só valem para este bloco de países, malgrado sejam utilizadas para servir de parâmetro para elaboração de legislações de outros países.

É importante mencionar que a Comissão Europeia, preocupada com os novos desafios impostos pela evolução tecnológica e, consequentemente, pelo aumento de partilha de dados pessoais, resolveu elaborar proposta de reforma para o novo quadro jurídico de proteção de dados pessoais neste bloco de países, apresentando versão final em 25 de janeiro de 2012. Duas propostas foram englobadas: a primeira seria a elaboração de um regulamento geral sobre proteção de dados pessoais e a segunda seria de uma nova Directiva do Parlamento Europeu e do Conselho para a proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção e repressão de infrações penais ou de execução de sanções penais.

Registre-se que até 2016, a Diretiva 95/46/CE era considerada o principal instrumento em matéria de proteção de dados pessoais na União Europeia. No entanto, a rápida evolução tecnológica ocorrida nos últimos tempos, com um grande aumento na coleta e compartilhamento de dados pessoais, fez surgir a necessidade de adaptação desta normatização aos novos desafios à proteção de dados. Observa-se ainda, uma grande fragmentação em relação a esta matéria nos Estados-membros, levando a certa insegurança jurídica.

A ideia de se elaborar um regulamento surgiu da consciência de que a ausência de regras comuns no âmbito da União Europeia criaria o risco de se ter diversos níveis de proteção nos Estados-membros, acarretando conflitos entre Estados que aplicam regras diferentes. A proposta de regulamento resume-se em três pontos específicos: a) as novas obrigações e responsabilidades das empresas; b) os novos direitos dos cidadãos titulares de dados pessoais e; c) os novos poderes das Autoridades de proteção de dados pessoais.

Em relação às Autoridades de controle, ampliam-se as suas funções no que concerne a cooperação mútua entre si e com a Comissão, tendo sido atribuída uma nova competência, denominada balcão único, criando-se ainda, o Comitê Europeu para a proteção de dados pessoais.

Ressalta-se que a implementação de tal proposta de regulamento harmoniza, atualiza e moderniza os princípios estabelecidos pela Diretiva 95/46, assim como propõe também um instrumento que seja aplicado diretamente ao cidadão [25].

Diferentemente da Directiva 95/46/CE, que estabelecia diretrizes para que cada Estado- Membro da União Europeia adotasse sua própria legislação, o GDPR foi desenvolvido com o objetivo de harmonizar as leis de proteção de dados dos países da União Europeia, sendo aplicável a todos Estados-membros.

A GDPR trará impactos significativos ás empresas brasileiras, na medida em que sua jurisdição torna-se extraterritorial, ou seja o referido regulamento não se limita somente a empresas localizadas na União Europeia.

[25] O Novo Regulamento UE 2016/679 do Parlamento Europeu e do Conselho, de 27/04/2016 entrou em vigor em maio de 2018, revogando a Directiva 95/46/CE. Disponível em https://www.cncs.gov.pt/content/files/regulamento_ue_2016-679_-_protecao_de_dados.pdf. Acesso em: 09/07/2018.

4

O controle de dados pessoais no direito brasileiro

O controle de dados pessoais na ordem jurídica nacional se apresenta de forma indireta. No Brasil, até 2018, não havia um marco regulatório específico de proteção de dados pessoais, mas tão somente previsões genéricas na Constituição Federal e leis especiais, que tratam apenas de forma superficial tal temática.

Dessa forma, defende-se neste trabalho, a importância de lei específica de proteção de dados pessoais, como instrumento para tutela da privacidade informacional, tendo em vista que com os avanços na área da tecnologia de informação e comunicação, a privacidade dos indivíduos restou fragilizada e mais exposta a ameaças e violações.

Reafirma-se o direito do indivíduo de ter o controle sobre as suas informações pessoais que estejam em poder de bancos de dados públicos e privados, o que se consubstancia no poder de consentimento para o tratamento de dados. Por intermédio do consentimento e da autonomia da vontade se pode estruturar uma disciplina que harmonize os interesses conflitantes.

O panorama jurídico nacional até 2018 não se mostrava suficiente e satisfatório para uma efetiva tutela da privacidade informacional, posto que os instrumentos jurídicos disponíveis até então não tratavam especificamente da tutela de dados pessoais, tendo em vista que a privacidade informacional tem um caráter muito mais especifico do que outros desdobramentos deste direito da personalidade.

Como foi visto anteriormente, a evolução tecnológica foi responsável pelo aumento das possibilidades de escolha do indivíduo, com reflexos diretos na personalidade, e mais especificamente na privacidade, imagem e identidade das pessoas. Com isso, o consentimento passou a ser um instrumento de escolha individual e de exercício da sua autonomia privada.

Nesse capítulo, analisar-se-ão os instrumentos normativos nacionais postos à disposição do indivíduo para a tutela de dados pessoais, com o objetivo de se verificar se os mesmos se mostram satisfatórios para uma efetiva proteção da privacidade informacional. Pretende-se, ainda, fazer um estudo crítico-reflexivo acerca da Lei Geral de Proteção de dados Pessoais no Brasil – Lei 13.709, de 14 de agosto de 2018.

4.1 A proteção constitucional e infraconstitucional de dados pessoais no Brasil

A disciplina constitucional sobre a regulamentação da proteção de dados pessoais aproxima-se mais do modelo norte-americano do que do s*tandart* europeu. A legislação do direito *anglo-saxão* tinha como princípio que o que não era expressamente proibido seria permitido. Já o modelo *alemão*, firmava o entendimento de que toda a atividade de tratamento de dados pessoais seria proibida, se não fosse permitida expressamente.

Ao tratar dos dados pessoais, o constituinte brasileiro dispôs sobre a dupla esfera do direito à intimidade. Como, liberdade positiva e como liberdade negativa, ao tutelar a inviolabilidade do sigilo dos dados, no art. 5º, XII e o *Habeas Data,* no seu art. 5º, LXXII, respectivamente. No entanto, deixou uma lacuna relativamente aos contornos daquilo que representa o sigilo dos dados (SAMPAIO, 1998, p. 548).

Muito se discutiu acerca do tratamento dispensado aos dados pessoais na Constituição Federal vigente. Para alguns autores, a

disciplina constitucional sobre a matéria se fez de forma muito tímida, sem detalhar as etapas do tratamento de dados, mas tão somente a alguns dos seus aspectos. Porém, não seria tarefa do legislador constituinte detalhar a proteção de dados. Ficaria a cargo da legislação infraconstitucional e dos intérpretes do direito a função de regulamentar o sistema de proteção de dados pessoais.

A proteção de dados pessoais decorre da tutela da privacidade, protegida em conjunto com a intimidade, no art. 5°, X da Constituição brasileira. No entanto, não se limita por esta, na medida em que há previsão de um leque de garantias constitucionais no ordenamento brasileiro extensível à matéria.

Nos dias atuais, o instrumento de maior relevância para a proteção de dados pessoais no Brasil é *Habeas Data,* criado pela Constituição de 1988 e regulamentado posteriormente pela Lei n. 9507/97. Mais recentemente foi aprovada normatização que trata dos direitos e deveres dos usuários da internet, Lei n. 12.965/2014, denominada Marco Civil da Internet, que trata de forma genérica da proteção de dados pessoais. As duas legislações serão estudadas nos tópicos subsequentes.

Todavia, antes de adentrar a análise mais aprofundada destas normatizações, faz-se necessário tecer algumas considerações acerca do tratamento constitucional concedido aos dados. O sigilo de dados pressupõe coleta, armazenamento e elaboração de dados, mas não se trata da sua comunicação ou transferência a terceiros (SAMPAIO, 1998, p 548).

Ferraz Junior (1993, p.446) entende que entre as expressões "sigilo" e "dados" deve-se colocar a comunicação, ou seja, permite-se a coleta, o armazenamento, a elaboração e a comunicação a terceiros.

No entanto, na forma como foi colocada por Ferraz Junior (1993), a interpretação mais adequada não seria esta, isto porque o dispositivo constitucional em comento pretende proteger a inviolabilidade do segredo de dados, no qual se inclui a proibição

de comunicação a terceiros, bem como a proibição de interceptação por quem quer que seja.

É preciso entender que no sentido usual, a expressão "dados" significa informações. Em sentido mais técnico, o termo "dados" implica aquela informação que passou por algum tipo de tratamento. Nesse sentido, o sigilo de dados diz respeito ao sigilo das informações tratadas de forma automatizada. Todavia, deve ter um perfil nominativo, para possibilitar identificar direta ou indiretamente o seu titular.

Em outras palavras, a inviolabilidade de dados diz respeito a sua não utilização de forma desleal, ou seja, sem o conhecimento e/ou consentimento do seu titular. Essa lealdade deve ser aferida após a ocorrência do fato, já que não se estabeleceu um regime de autorização, fazendo-se uma análise da adequação dos meios aos fins e dos fins ao direito (SAMPAIO, 1998, p. 550).

Obviamente que, nem todo tratamento de informação precisa passar pelo consentimento do seu titular. Como já se demonstrou no capítulo anterior, nos casos em que houver interesse social ou público relevantes em conflito, essas informações poderão circular, mas sempre se garantindo o núcleo essencial do direito à privacidade e à intimidade, como por exemplo, os dados sensíveis.

Observa-se que além da previsão constitucional existente no que se refere a dados, há diversas disposições esparsas, que podem ser encontradas no âmbito do direito civil, do direito processual e no direito penal, bem como disposições de perfil comercial e tributário. E mais, muitas destas normativas foram elaboradas em período anterior à Constituição de 1988, como por exemplo, a Lei n 7.232/84, que dispõe sobre a Politica Nacional de Informática, prevendo a estruturação e exploração dos bancos de dados.

O Código de Defesa do Consumidor, Lei n. 8.078/90 assegurou ao consumidor no seu art. 43, o acesso às informações pessoais em cadastros, fichas e registros de dados e de consumo arquivados, limitando a permanência desses registros pelo prazo

máximo de cinco anos ou até a prescrição da ação de cobrança (o que ocorrer primeiro).

O legislador consumerista demonstrou preocupação com o equilíbrio das relações de consumo, por meio da imposição de limites ao uso de informações de consumidores pelos fornecedores. O uso de informações por parte do fornecedor se mostra como fator de segurança, ou mesmo para desenvolver técnicas comerciais para incremento da sua atividade. No entanto, é necessário que se estabeleça limites, para que o consumidor não perca sua liberdade de escolha, assim como não seja discriminado com o uso destas informações.

Pela análise do Código de Defesa do Consumidor, anteveem-se alguns princípios de proteção e dados pessoais compatíveis com as relações de consumo, os quais foram estudados no capítulo anterior. Por esta razão, aplicam-se apenas as relações específicas, sem integrarem um sistema geral de proteção de dados pessoais, muito embora sirvam como parâmetros para outras situações, que não sejam relações de consumo.

Pode-se citar o princípio da finalidade em nosso ordenamento, através da aplicação da boa-fé objetiva e da própria garantia da privacidade, pois os dados fornecidos pelo consumidor deverão ser utilizados somente para os fins que para os quais foram coletados (DONEDA, 2006, p. 339).

Destaca-se ainda, que a legislação infraconstitucional dividiu a matéria do sigilo de dados em: sigilo bancário, sigilo fiscal e sigilo das comunicações telefônicas. A lei n. 4.595/64, art. 38, recepcionada pela Constituição de 1988, permitia a quebra do sigilo bancário por autorização judicial, por determinação da CPI ou requisição do Ministério Público quando objeto de investigação criminal.

No entanto, esse dispositivo foi revogado pela Lei Complementar n. 105/2001. Com isso, admitiu-se a possibilidade de autoridades e agentes fiscais tributários da União, Estados, Distrito Federal e Municípios analisarem documentos, livros e

registros de instituições financeiras, quando houver sido instaurado processo administrativo ou procedimento fiscal. Não obstante, o resultado da pesquisa deve permanecer conservado em sigilo.

Respeitados os direitos individuais, é facultada à administração tributária identificar o patrimônio, os rendimentos e as atividades econômicas do contribuinte, desde que individualizados o investigado e o objeto da investigação. Ressalta-se que com o advento da Lei Complementar n. 104/2001 ficou permitida a divulgação desses dados pela Fazenda Pública por simples solicitação da autoridade administrativa no interesse da Administração Pública, desde que comprovada a instauração de processo administrativo.

Alguns autores, porém, entendem que essa liberalidade da LC n. 104/2001 é inconstitucional, por violar a ordem constitucional que estabelece que a quebra do sigilo só se dará por determinação judicial. O Supremo Tribunal Federal ao se manifestar sobre esta matéria em sede de Recurso Extraordinário nº 389.808[1], decidiu pela necessidade de autorização judicial para a

[1] O referido caso se deu com comunicado feito pelo Banco Santander à empresa GVA Indústria e Comércio S/A, informando que a Delegacia da Receita Federal do Brasil – com amparo na Lei Complementar nº 105/01 – havia determinado àquela instituição financeira, em mandado de procedimento fiscal, a entrega de extratos e demais documentos pertinentes à movimentação bancária da empresa relativamente ao período de 1998 a julho de 2001. O Banco Santander cientificou a empresa que, em virtude de tal mandado, iria fornecer os dados bancários em questão. Por esta razão, a empresa ajuizou ação, que culminou com o julgamento do RE no Supremo Tribunal Federal contra acórdão proferido pelo Tribunal Regional Federal da 4ª Região, que permitiu

"o acesso da autoridade fiscal a dados relativos à movimentação financeira dos contribuintes, no bojo do procedimento fiscal regularmente instaurado". Para a empresa GVA, "o poder de devassa nos registros naturalmente sigilosos, sem a mínima fundamentação, e ainda sem a necessária intervenção judicial, não encontram qualquer fundamento de validade na Constituição Federal". Afirma que foi obrigada por meio de Mandado de Procedimento Fiscal a apresentar seus extratos bancários referentes ao ano de 1998, sem qualquer autorização judicial, com fundamento apenas nas disposições da Lei nº 10.174/2001, da Lei Complementar 105/2001 e do Decreto 3.724/2001, sem qualquer respaldo constitucional. O Relator Min. Marco Aurélio votou pelo provimento do recurso, tendo como fundamento a dignidade da pessoa humana e o principio da inviolabilidade das informações, como forma de garantir segurança e estabilidade para as relações, sendo necessário assegurar a privacidade das pessoas. Esta regra, na opinião do Relator só poderá ser mitigada por ordem judicial. Jul. em 15/12/2010, DJ de 10/05/2011. Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=168193. Acesso em: 01 de jul. 2014.

quebra ou em razão de ato da CPI. No entanto, o posicionamento definitivo do STF sobre a referida matéria foi no sentido, por maioria de votos – 9 a 2 – , prevaleceu o entendimento de que a norma não resulta em quebra de sigilo bancário, mas sim em transferência de sigilo da órbita bancária para a fiscal, ambas protegidas contra o acesso de terceiros. A transferência de informações é feita dos bancos ao Fisco, que tem o dever de preservar o sigilo dos dados, portanto não há ofensa à Constituição Federal.

No concernente à quebra do sigilo das comunicações telefônicas, sua autorização se fará nas hipóteses e na forma que a lei estabelecer. Sempre para os fins de investigação criminal ou instrução processual penal, nos termos da lei n. 9296/96.

4.2 O *Habeas Data* no direito brasileiro

O *Habeas Data* é uma garantia criada pela Constituição de 1988, que influenciou legislações latino-americanas. Não chegou a surpreender, porque o aparecimento deste remédio também foi resultante de fatores geopolíticos. A adoção do instituto por muitos países latino-americanos, ao fato de que na década de 1980, credita-se ao fim de alguns regimes ditatoriais que utilizavam as informações de modo excessivamente autoritário.

O problema naquela época, não estava apenas no uso das informações, mas sim no abuso à sua utilização. Diferentes organismos armazenavam informações sobre as pessoas, sobretudo os órgãos de segurança, que perseguiam os adversários[2].

[2] Com o advento do golpe militar de 1964, foi produzida farta documentação pelos órgãos de informação, que integram hoje o Centro de Referência das Lutas Politicas – Memórias Reveladas, criado em 2009 pela Casa Civil da Presidência da República, sob a coordenação do Arquivo Nacional. O banco de dados disponível no portal *Memórias Reveladas* oferece informações sobre as investigações e diligências policiais-militares, cassações de direitos, controle individual de pessoas, associações e organizações tidas como suspeitas, dentre outros assuntos. A disponibilização deste acervo constitui um marco na democratização do acesso à informação, bem como serve de instrumento de formação da cidadania. (REDE DE INFORMAÇÕES E CONTRAINFORMAÇÕES DO REGIME MILITAR NO BRASIL. Disponível em: http://www.arquivonacional.gov.br. Acesso em: 02 de jul. 2014).

A denominada *comunidade de informação* passou a constituir um poder paralelo e agressivo (BARROSO, 1998, p. 211), em sobreposição por vezes ao poder institucional. Valendo-se, inclusive, de provas ilícitas.

Dessa forma, o instituto do *Habeas Data* foi criado em momento oportuno, no qual não se concebiam mais as violações perpetradas contra direitos da personalidade, sobretudo, contra o direito à privacidade e à intimidade das pessoas. Esse remédio constitucional teve como objetivo possibilitar ao cidadão o conhecimento direto de informações que lhe diziam respeito, bem como, se necessário retificar tais dados, em caso de incorreção ou inexatidão.

Pode-se afirmar que o *Habeas Data* é uma das ações que constituem o rol de instrumentos para garantia de direitos individuais e coletivos. A sua posição no ordenamento deve ser entendida como uma reação para consolidar as bases democráticas e evitar o retorno ao regime ditatorial (DONEDA, 2006, p. 332-333), no momento em que a sociedade e o próprio ordenamento estavam se recompondo de um período de ditadura e diversas liberdades individuais vinham sendo suprimidas.

A doutrina discutia se o aparecimento do *Habeas Data* foi influenciado pelo pensamento jurídico europeu ou norte-americano, isto porque na época de sua inauguração, no Brasil, aqueles países já possuíam experiência na matéria. Todavia, Doneda (2006, p. 328) lembra que as consequências derivadas das tecnologias na América Latina se apresentam, de forma geral, defasadas e atenuadas em relação aos países desenvolvidos. Acrescente-se a isso, o fato de que naquela época faltava um modelo bem estruturado e claro para servir de exemplo, pois as experiências europeias se desenvolviam isoladamente.

Sampaio (1998, p 548) entende que o modelo brasileiro de regulamentação de dados pessoais se aproxima mais do *standart* norte-americano do que do modelo restritivo europeu. Como se afirmou no tópico anterior, o modelo europeu se mostrou mais

rígido, sob a regra de que todo o processamento de dados pessoais seria proibido, se não fosse expressamente permitido.

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

A Constituição Federal de 1988, no art. 5°, LXXII, dispõe que:

> Conceder-se-á *habeas data:* a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para retificação de dados, quando não se prefira fazê-lo por sigiloso, judicial ou administrativo (BRASIL, 1988).

Quando do surgimento deste remédio constitucional pela Constituição brasileira vigente, muito se questionou se realmente haveria necessidade de se criar uma nova garantia processual, para além do Mandado de Segurança. Até mesmo porque quando da entrada em vigor da Carta de 1988, entendeu-se que tal instituto seria imediatamente aplicável, uma vez que, na falta de norma regulamentadora, seria possível aplicar aquelas normas atinentes ao Mandado de Segurança.

Somente após nove anos da promulgação da Constituição de 1988, foi editada a chamada lei do *Habeas Data,* Lei n. 9.507/97 que passou a regular o direito de acesso ás informações e disciplinar o rito processual desse remédio constitucional.

Após o advento da Lei n. 9.507/97, não só foi implementada a forma de obtenção dos direitos assegurados nas alíneas “a” e “b”, do inciso LXXII, do art. 5°, como também foi delineado o

procedimento do *Habeas Data,* caso seja necessário o ingresso no poder judiciário.

Percebe-se que o instituto ora em estudo, pretende garantir os direitos de intimidade e, de forma mais ampla, os direitos à informação, devidamente reconhecidos pela Constituição Federal de 1988. O art. 5º, X, estabelece: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". O inciso XIV do mesmo dispositivo dispõe que "é assegurado a todos o acesso à informação e o resguardado o sigilo da fonte, quando necessário ao exercício profissional" (BRASIL, 1988).

Pode-se afirmar que a obtenção, o armazenamento e a manipulação de dados sobre o indivíduo constituem uma verdadeira ameaça não só à sua privacidade e intimidade, como também à própria liberdade individual. Tal violação a direitos valiosos da personalidade humana assumiu grandes proporções a partir da evolução nas tecnologias de informação e comunicação ocorridas nos últimos anos. O direito à intimidade e o direito à privacidade não estariam devidamente protegido se não fosse a criação de instrumentos processuais que garantissem a efetividade destes direitos.

Não obstante a importância deste instrumento processual para a tutela dos direitos à intimidade e à privacidade, ainda há comumente violações perpetradas contra a privacidade informacional, mais especificamente as informações pessoais constantes em bancos de dados. O remédio constitucional ora analisado somente se aplica quando o indivíduo deseja obter ou retificar informações a seu respeito. Na verdade, não permite ao seu titular qualquer controle sobre a manipulação e tratamento das informações que as empresas públicas ou privadas detenham a seu respeito.

É justamente nesse ponto que reside o problema acerca da privacidade informacional: a falta de controle do titular sobre essas

informações. Esse fato é bastante corriqueiro no mundo globalizado em que se vive. Muitas vezes, o indivíduo disponibiliza seus dados às empresas privadas, que formam verdadeiros cadastros, com o objetivo de favorecer a celebração de contratos de consumo, ou a divulgação de seus produtos e serviços. Posteriormente, porém, essas organizações transmitem tais informações a outras empresas, sem o conhecimento e a autorização do seu titular, facilitando a lesão ou ameaça à sua intimidade e á sua privacidade.

Com o advento da Lei n. 9.507/97, além da previsão constitucional das alíneas do art. 5°, LXXII, o legislador infraconstitucional estabeleceu uma terceira hipótese para cabimento do *Habeas Data,* qual seja "para anotação nos assentamentos do interessado, de contestação ou explicação sobre dado verdadeiro mas justificável e que esteja sob pendência judicial ou amigável" (art. 7°, III).

Naquela época foi objeto de discussão se tal previsão infraconstitucional seria inconstitucional, pelo fato de ter o legislador ordinário previsto hipótese não garantida no Texto Constitucional. No entanto, a ampliação do objeto desta garantia constitucional, na opinião de Bueno (2012, p. 71) não viola o comando constitucional por ser ampliativo do direito e da garantia minimamente estabelecidas no Texto Maior.

Observa-se que a previsão infraconstitucional do inciso III, do art. 7° pode revelar-se mais frágil que aquelas previsões constitucionais. Isto porque poderá ser alterada ou mesmo suprimida por lei ordinária, já que não se trata de comando constitucional.

Outra questão da lei em análise que merece destaque está no art. 1°, parágrafo único, estabelecendo-se que as informações obtidas, retificadas ou anotadas devem ser de entidades de caráter público. Enquadra-se em tal perfil, todo banco de dados que contenha informações que sejam ou possam ser transmitidas a terceiros ou que não seja de uso privativo do órgão.

Note-se que o caráter público das informações não se refere ao sentido estatal. A lei se utiliza do termo público em sentido mais amplo do que aqueles dados manuseados pela administração pública, sendo absolutamente indiferente se a pessoa detentora dos dados for pessoa de direito público ou privado.

Todavia, qualificar os dados como de caráter público em virtude de transmissibilidade a terceiros, restringe um pouco o campo de atuação de sua proteção por *habeas data*. É possível identificarem-se bancos de dados de empresas que não têm por objetivo a transmissão de informações a terceiros. Tome-se como exemplo, o caso de uma pessoa que, desejando adquirir determinado bem, precise preencher um cadastro com todos os seus dados, para celebração do contrato. Assim, mais uma vez se demonstra que a referida legislação não se mostra como suficiente para a tutela efetiva da privacidade informacional.

Nesse sentido, percebe-se que a ideia central do referido instituto era de que se a entidade se limita a armazenar dados para seu próprio e exclusivo uso, não caberia *Habeas data, p*or não violar o dispositivo que estabelece que o ente seja governamental ou de caráter público. O exemplo típico de entidade de caráter público são os serviços de proteção ao crédito, em que os registros se destinam à orientação dos usuários.

Foi objeto também de controvérsias o requisito da necessidade da fase pré-judicial. O indivíduo que deseja impetrar *Habeas Data,* necessita se dirigir primeiramente à entidade detentora do banco de dados, sendo a via judicial aberta apenas na hipótese de recusa ao acesso ou à retificação de dados.

A Lei 9.507/07 é clara a esse respeito, dispondo no seu ar. 2º que "o requerimento será apresentado ao órgão, ou entidade depositária do registro ou banco de dados e será deferido ou indeferido no prazo de 48 (quarenta e oito) horas". (BRASIL, 2007)

Dessa forma, toda vez que o indivíduo pretender obter, retificar ou anotar informações a seu respeito deverá fazer a solicitação diretamente à entidade pública ou privada detentora das

informações, devendo o seu pedido ser deferido ou indeferido no prazo de 48 horas. Nas vinte e quatro horas seguintes ao deferimento ou indeferimento seguintes, o interessado deverá ser informado da decisão que, desejando retificá-los, deverá solicitar com documentos comprobatórios.

O que se observa pela leitura da lei em comento é que após a entrada do requerimento perante a entidade, a mesma terá o prazo de dez dias para retificar eventual incorreção nos dados, bem como para proceder a anotação se for o caso.

Não obstante a divergência ocorrida em torno do exaurimento da esfera administrativa, a doutrina e jurisprudência dominantes inclinaram-se no sentido de que se não houver recusa, carece ao impetrante o interesse processual, o que se justifica por uma questão de economia processual. Para que ocupar o judiciário com uma questão que pode ser resolvida no âmbito administrativo?

O interesse de agir, segundo Bueno (2012, p. 76) só surge quando frustradas eventuais tentativas do interessado de obter, retificar ou anotar informações a seu respeito. Sem que haja recusa expressa ou tácita não há necessidade de se impetrar *Habeas Data,* orientação que já fora sumulada pelo Superior Tribunal de Justiça – Súmula 02 "Não cabe o habeas data se não houve recusa de informações por parte da autoridade administrativa".

Nesse sentido, não se trata da obrigatoriedade de esgotamento da via administrativa, mas tão somente otimizar a prestação de serviços tida como função pública pelo Estado ou por quem detém informações para uso de terceiros, ou seja, averiguar a necessidade ou não de ingresso de ação judicial de *habeas data.*

A fase judicial do *habeas data* está prevista no art. 7º e ss da Lei n. 9.507/97. Logo o primeiro dispositivo prevê as três hipóteses de cabimento da referida ação: I – pedido de informações relativas à pessoa do impetrante; II – pedido de retificação de dados inexatos e, III – pedido de anotação nos respectivos assentamentos. Como já mencionado, a ampliação desta terceira hipótese não merece censura do ponto de vista constitucional, isto porque a referida lei

não restringiu o campo de atuação do citado remédio constitucional (BRASIL, 1997).

Logo em seguida, no art. 8º da citada Lei, o legislador estabeleceu a obrigatoriedade da chamada prova pré-constituída, ao exigir junto com a petição inicial, a prova: a) da recusa de acesso às informações, ou decurso de mais de dez dias sem resposta; b) da recusa em se fazer a devida retificação em caso de incorreção da informação; ou c) da recusa em proceder à anotação nos assentos do banco de dados, conforme preceitua o § 2º do art. 4º da referida lei.

Nesse contexto, Doneda (2006, p. 337) observa que um sistema de proteção de dados pessoais que tenha como instrumento principal o recurso a uma ação judicial, que só poderá ser intentada após inafastável périplo administrativo, não se apresentam como adequadas as exigência da matéria, isto porque o sistema de tratamento de dados pessoais se mostra cada vez mais "em branco", sem o conhecimento do interessado.

Nessas situações, o indivíduo terá que recorrer à via administrativa, em que o não atendimento não acarretará nenhuma penalidade à entidade detentora das informações e, somente no insucesso dessa tentativa, poderá ajuizar ação de *Habeas Data,* que ao contrário do *Habeas Corpus,* necessita da presença de advogado.

Somente a própria pessoa titular das informações terá legitimidade ativa para impetrar tal ação judicial, o que fica demonstrado quando da leitura da alínea *a* do inciso LXXII alude a "informações relativas à pessoa do impetrante". Assim, não se admite que qualquer outra pessoa pretenda obter informações de terceiros, via *habeas data*. Quando o legislador se referiu à "pessoa", não estava indicando como legitimadas apenas as pessoas físicas, mas também as pessoas jurídicas.

O procedimento previsto na Lei do *Habeas Data* segue, em linhas gerais, o padrão da Lei do Mandado de Segurança, o que se justifica pela patente afinidade entre os dois institutos, implicando

que nos casos omissos da Lei n. 9.507/97, deve-se aplicar a Lei do Mandado de Segurança – 12.106/09.

Verifica-se que a parte processual da lei do *Habeas Data* é uma cópia da lei do Mandado de Segurança, Lei n. 1.533/51, vigente na época. Tal fato faz constatar que o legislador da primeira lei citada perdeu a oportunidade de inovar, considerando as diversas mudanças ocorridas no processo civil no decorrer dos anos que separaram as duas leis. Cite-se como exemplo, o fato de ambas as legislações não se preocuparem em dizer quem seria considerado "réu" na ação, se aquele que pratica o ato impugnado ou a pessoa jurídica que está vinculada.

A criação de mecanismos como o *habeas data* para tutela das informações pessoais se mostra de pouca eficácia diante da realidade fática, isto porque dificilmente o cidadão exercerá algum controle sobre estas informações pessoais constantes nos chamados "dossiês digitais", denominação dada por Solove (2004, p. 143).

Deve-se entender que os problemas relativos à coleta, armazenamento e uso de informações por bancos de dados são totalmente diferentes daqueles que se referem à vigilância governamental, como naquela noção de sociedade de controle baseada na obra de George Orwell, em 1984. A metáfora do "Grande irmão" tem como objetivo o comportamento e controle social e não os danos causados pela utilização das informações. Na verdade, os chamados dossiês digitais, construídos pelas empresas têm como objetivo estimular o consumo e não oprimir (LEONARDI, 2012, p. 202).

O grande problema que se apresenta com os dossiês digitais, é justamente a criação de perfis das pessoas, construídos a partir de informações, antes esparsas, com o objetivo de transmiti-las a outras empresas, isto é, desvirtuando a finalidade para a qual os dados foram disponibilizados, sem o conhecimento e autorização do seu titular.

Em outro sentido, Solove (2004, p. 228-230, E-book) esclarece que não se trata apenas da perda de controle das informações pessoais, nem tão pouco de um plano de dominação do "Grande Irmão". Para o referido autor, o problema é que o processo burocrático é descontrolado e o uso das informações tem efeitos palpáveis, considerando que os referidos dossiês digitais são utilizados por empresas e por governos para tomar decisões sobre indivíduos, que muitas vezes não têm ao menos conhecimento de tal fato.

Percebe-se quanto de obstáculos o indivíduo terá que enfrentar para ajuizar uma ação de *Habeas Data*. Em primeiro lugar, ele tem que tomar conhecimento de que existem bancos de dados contendo suas informações pessoais, pois na maioria das vezes não dispõe desta informação. Após tomar conhecimento, deverá se dirigir à entidade governamental ou de caráter público, para obter, retificar ou fazer anotações a respeito de seus dados. Somente com a recusa de tais pedidos, poderá impetrar este remédio constitucional.

Acrescente-se que, não obstante a ação de *Habeas Data* ser gratuita, isentando o impetrante das custas processuais, terá o interessado que contratar advogado para ajuizar a ação, ao contrário do que ocorre com a ação de *Habeas Corpus*. Registre-se que tal requisito já se mostra como fator de desestímulo para o cidadão, o que é comprovado pelo número de ações de *Habeas Data* ajuizadas no Brasil.

Alguns autores defendem que a Lei n. 9.099/95 seja modificada, possibilitando o ingresso deste remédio constitucional nos Juizados Especiais Cíveis, pelo próprio interessado, sem a necessidade de assistência de advogado, nas causas de até 20 (vinte) salários mínimos (LEONARDI, 2012, p. 206).

Nesse sentido, observa-se que os diversos mecanismos de tutela previstos na Constituição Federal, no Código de Defesa do Consumidor e na Lei 9.507/97 ainda são insuficientes para uma tutela efetiva da privacidade informacional. Necessário se faz, frise-

se novamente, uma tutela específica deste direito, por meio de legislação de proteção de dados pessoais, com a criação de órgão de controle ou autoridade administrativa independente, a exemplo do que se tem nos países da União Europeia, conforme orientação da Diretiva 95/46/CE, bem como nos Estados Unidos, com a *Federal Trade Comission, q*ue exerce o papel de controle e fiscalização de dados pessoais.

Na verdade, o *Habeas Data* é um produto do seu tempo, criado para uma necessidade específica: a de obter, retificar ou fazer anotação de informação pessoal. Hoje, enfrenta o desafio de demonstrar sua aplicabilidade e eficácia, diante de novos recursos da tecnologia de informação e comunicação.

4.2.1 O Habeas Data em outros países da América Latina

Cumpre analisar, nesse momento, a influência deste remédio constitucional em outros países da América Latina, para entender e identificar as diversas características deste instituto nos diversos países que previram expressamente o *Habeas Data,* mesmo com outra denominação.

Pode-se encontrar o referido instituto na Colômbia, Paraguai, Peru, Argentina e Equador, bem como há previsão expressa também na Constituição da República Bolivariana da Venezuela, que estabelece no seu art. 281, dentre as atribuições do defensor público, *in verbis: "*(...) 3. Interponer las acciones de inconstitucionalidade, amparo, habeas corpus, habeas data y lás demás acciones o recursos necesarios para ejercer las atribuciones señaladas em los ordinales anteriores, cuando fuere procedente de conformidade com la ley".

A Colômbia previu o referido instituto na sua Constituição de 1991, sendo a primeira a tratar desta garantia após o Brasil, no entanto, não o previu como ação, reconhecendo tão somente garantias relacionadas com a proteção de dados pessoais, conforme se percebe da leitura do seu art. 15:

> Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacer-los respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y em archivos de entidades públicas e privadas.

O legislador constituinte não utilizou expressamente o nome *Habeas Data,* entretanto, a doutrina e a jurisprudência colombiana logo trataram de lhe dar o referido nome.

Na Argentina, pode-se identificar a experiência mais rica em termos da garantia de proteção de dados pessoais, isto porque mesmo antes da previsão constitucional do *habeas data,* havia a possibilidade das províncias legislarem sobre a matéria, sendo que muitas efetivamente legislaram antes e depois da inovação trazida pela Constituição Nacional.

Inicialmente, a Constituição Nacional, no seu art. 19 tutelava apenas a vida privada, que posteriormente foi regulamentado pela Lei n. 21.173, estabelecendo um direito subjetivo à intimidade. No entanto, em 1994 a referida Constituição passou por reforma, com uma previsão específica sobre dados pessoais, no seu § 3°, do art. 43:

> Todas persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidade, que consten em registros o bancos de datos públicos, o los privados destinados a provecer informes, y em caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencalidad o actualización de aquellos.

Convém lembrar que a mencionada previsão acabou sendo conhecida como *Habeas Data,* uma forma específica da chamada Ação de Amparo prevista no *caput* do art. 43 da Constituição Nacional, no entanto apresentando características bem mais amplas do que *Habeas Data* brasileiro.

Pode-se identificar alguma semelhança entre o instituto previsto na Argentina e no Brasil, como por exemplo, ambos têm aplicabilidade imediata. Entretanto, no caso argentino, parece ter logrado mais êxito, na opinião de Doneda (2006, p. 348), pelo fato de ter maior acolhimento pelos tribunais. Soma-se a isto, o fato de que logo após a previsão constitucional foi editada lei especifica para proteção de dados pessoais, muito embora tenha sido objeto de veto pelo poder executivo em 1996.

Não obstante sua aplicabilidade imediata, no caso argentino, a proteção de dados pessoais carecia de legislação específica, o que fez com que várias províncias editassem suas próprias leis de proteção de dados pessoais. E, em 2000, o governo argentino resolver promulgar a Lei n. 25.326/2000, que passou a regulamentar a ação de *Habeas Data,* tutelando especificamente os dados pessoais.

É interessante notar que no art. 29 da lei em comento, há uma iniciativa pioneira na América Latina: a criação de um órgão de controle, o *Dirección Nacional de Protección de Datos Personales* – DPDP. Dentre as suas funções, registram-se não só a assistência jurídica, mas também a competência para regulamentar e manter o registro para notificação de operações relacionadas a bancos de dados. Este órgão goza de autonomia funcional e está vinculado à estrutura do Ministério da Justiça, sendo seus membros indicados pelo Poder Executivo.

Observa-se que a lei do *Habeas Data* argentina de 2000 acabou tratando de forma mais específica a proteção de dados pessoais, criando inclusive, órgão fiscalizador, diferente do tratamento dado pela lei brasileira, que se restringiu ao direito de obter, retificar ou complementar informações pessoais.

Pode-se constatar que após a previsão constitucional do referido instituto, em 1988 no Brasil, houve uma disseminação de tal ação nos países da América Latina, tendo como forte contribuição a tentativa de superação do período da ditadura militar que assolava vários países naquela época. Nesse contexto, o

Habeas Data representaria uma forma de assegurar um direito ao conhecimento de informações a respeito do cidadão, simbolizando assim uma mudança no paradigma anterior.

Muito embora se reconheça a importância do referido instituto nos países da América Latina, sobretudo no caso brasileiro, não se pode olvidar a necessidade de adaptação de uma ordem de problemas substancialmente diversa. Trata-se da proteção de dados pessoais, já que o mencionado remédio constitucional não se mostra como opção satisfatória para resolução de problemas ligados à sociedade de informação.

Parece estranho o Brasil ter sido o pioneiro na criação da legislação do instituto do *Habeas Data* e ter demorado tanto tempo para ter uma normatização específica sobre dados pessoais. Observa-se que, comparativamente com os demais países da América Latina, a legislação brasileira é a menos desenvolvida, isto porque somente em 2018, foi aprovada lei de de proteção de dados pessoais.

A legislação infraconstitucional vigente não se mostra compatível com uma leitura constitucional dos interesses ligados à proteção de dados pessoais, necessitando de instrumentos adequados para sua atuação com o objetivo de proporcionar uma efetiva atuação da Constituição no que tange à tutela da personalidade (DONEDA, 2006, p. 358).

Antes de adentrar na análise específica dos projetos de lei de dados pessoais no Brasil, convém analisar a Lei 12.965/2014 - Marco Civil da Internet, para identificar a contribuição de tal normatização para a proteção de dados pessoais.

4.3 A importância do Marco Civil da Internet para proteção de dados pessoais

O Projeto de Lei n. 2.126/2011, denominado Marco Civil da Internet, estabeleceu princípios, direitos e deveres para o uso da internet no Brasil. Foi aprovado pelo Senado Federal em

22/04/2014, após tramitação na Câmara dos Deputados e, posteriormente convertida na Lei nº 12.965/2014.

A estrutura da presente lei está pautada em três pilares: a neutralidade, a privacidade e a liberdade de expressão. Prevista no art. 3º, IV e no art. 6º, a neutralidade impõe que todo conteúdo trafegado pela internet deve ser tratado de forma igual, navegando na mesma velocidade. Esse princípio garante livre acesso a qualquer tipo de informação. Para que haja discriminação ou exceções à neutralidade, necessário se faz decreto presidencial, após consulta do Comitê Gestor da Internet.

Assim, as operadoras de telecomunicações não podem fazer distinção de tráfego baseadas em interesses comerciais. Deve-se garantir que os dados possam ser acessados sem qualquer distinção no que se refere à origem ou conteúdo, pois os provedores da internet não podem fixar valores extras para que usuários participem de determinados serviços, por exemplo[3].

A privacidade é mencionada no art. 3º e no art. 7º, I, quando estabelecem os direitos do usuário no acesso à internet. Textualmente se afirma a inviolabilidade da intimidade e da vida privada, bem como a sua proteção e indenização por dano material ou moral decorrente de sua violação. Prevê ainda, no seu art. 8º que "A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet".

A privacidade das pessoas na era digital vem sendo há muito tempo ameaçada, no entanto, o governo brasileiro só passou a atentar para o fato após denúncias de espionagem dos EUA, conforme foi mencionado no capítulo anterior deste trabalho. Por

[3] Recentemente, a operadora de serviços Velox e banda larga da Oi foi multada pelo Ministério da Justiça por infrações às normas de defesa do consumidor. Esta condenação foi motivada em razão do serviço navegador disponibilizado aos consumidores. Foi constatado que a Oi em parceria com a empresa britânica Phorm estava desenvolvendo um software chamado "navegador", que mapeava o trafego de dados do consumidor na internet, traçando o seu perfil de navegação. Estes perfis eram comercializados com anunciantes, agências de publicidade e portais da *web.* (Matéria publicada no dia 24 de jul. 2014. Disponível em: http://www.migalhas.com.br. Acesso em: 24 de jul. 2014).

esta razão, houve certa "urgência" na aprovação desta lei, somando-se a este fato, o evento NetMundial[4]realizado aqui no Brasil, em que a Presidente Dilma Rousself pretendia utilizar a mencionada lei como "marca" da sua gestão no setor de tecnologia de informação.

Quando da aprovação da referida legislação, muito se discutiu se a liberdade de expressão não estaria sendo violada, diante de certas limitações impostas para a tutela da privacidade das pessoas. No entanto, percebeu-se que ambos os interesses (liberdade e privacidade) são direitos da personalidade preservados pela nova lei, embora passíveis de limitações. Afinal, nem mesmo a fundamentalidade de um direito o torna absoluto.

Conquanto a nova legislação aborde a temática da proteção de dados pessoais, não o faz de maneira detalhada e deixa a tarefa a cargo de ulterior lei específica. Ou seja, o legislador cuidou apenas de alguns aspectos da tutela dos dados pessoais. No art. 3°, III dispôs que a proteção dos dados pessoais é um dos princípios a ser observado para a disciplina do uso da internet. Garantiu a inviolabilidade e sigilo do fluxo de suas comunicações, no art. 7°, II. Também foi objeto de tutela a inviolabilidade das comunicações privadas armazenadas, salvo por ordem judicial.

No Marco Civil da Internet ficou assegurado no art. 7°, VIII, que os usuários da internet terão informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de dados pessoais, que somente poderão ser utilizados para as finalidades pelas quais foram coletados. Fica assegurado ainda no inciso VII "o não fornecimento a terceiros de seus dados pessoais, inclusive registro de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei".

[4] O evento Netmundial foi realizado em São Paulo nos dias 23 e 24 de abril de 2014. Trata-se de encontro para discutir o futuro da Governança da internet. Mais informações: Disponível em: http://www.netmundial.br. Acesso em: 20 de jul. 2014.

Veja-se que o consentimento assume lugar de destaque em tal regulação, estando intrincada a autodeterminação informativa, no poder de controle que o indivíduo deve ter de informações que lhe dizem respeito. Tais dados só poderão sair da esfera de controle do seu titular com a sua autorização.

Não é demais lembrar que o Marco Civil da Internet, ainda na fase de projeto, passou durante o processo legislativo por uma Comissão especial, composta por técnicos, juristas, acadêmicos, políticos e representantes de varias entidades com o objetivo de discuti-o, culminando com relatório sobre os debates estabelecidos.

No referido relatório, um dos pontos que chamou a atenção, independente de se ter uma legislação específica sobre proteção de dados pessoais, foi o direito à autodeterminação informativa, consubstanciada no controle das informações pessoais na internet, um direito garantido pela legislação em comento.

De fato, essa legislação não poderia ficar alheia à proteção de dados pessoais, muito embora não seja seu objetivo principal, no entanto, na ausência de legislação específica acerca desta matéria, o Marco Civil teve que antecipar algumas regras referentes ao tratamento de dados pessoais, até porque uma grande parte da utilização da w*eb* envolve a questão do uso de dados pessoais dos internautas.

Nesse sentido, observa-se que os s*ites* brasileiros utilizam os dados dos usuários de forma totalmente indiscriminada, não esclarecem nem informam de forma transparente o que acontecerá com as informações que lhes são solicitadas. Muitos *sites* de redes de lojas sequer informam que utilizam na sua política de segurança os chamados *Cookies,* ou quando informam não o fazem de forma clara e transparente.

Os denominados *Cookies s*ão arquivos no formato de texto, utilizados para armazenamento de dados, tendo como objetivo a personalização e otimização do usuário em determinado ambiente virtual, instalados de forma automática no disco rígido do

computador do usuário no momento da visita àquela página virtual (FOROUZAN, 2006, p. 854).

A questão gira em torno da relação dos *Cookies* com a privacidade. Na maioria das vezes, há o total desconhecimento por parte dos usuários que têm seus dados coletados e monitorados, situação que impossibilita o controle destas informações pelos seus titulares.

Nesse contexto, muito dificilmente o cidadão tem condições de perceber o risco que a coleta e o armazenamento de informações pessoais por empresas dotadas de meios sofisticados de tratamento de dados podem trazer para ele. Assim, o usuário deverá ser informado de forma clara e transparente acerca de todo o processo de tratamento de seus dados, pois somente ele terá o poder de autorizar a utilização destas informações.

No ano de 2000 já havia certa preocupação com a segurança na internet. Um grupo de estudos identificou a necessidade de um guia com informações sobre segurança que pudesse ser usado como referência pelos diversos usuários de Internet. Com isso, a pedido do Comitê Gestor da Internet no Brasil e sob supervisão do Centro de Estudos, Resposta e Tratamento de incidentes de segurança no Brasil - CERT.br, em julho do mesmo ano foi lançada a Cartilha de Segurança para Internet (CGBLBR, 2012, p. 05)

Em 2003, a Cartilha passou por uma revisão geral, incluindo-se novos tópicos, como também facilitando sua leitura e a localização a assuntos específicos. A referida Cartilha foi completamente reescrita, dando origem a versão 2.0. Entretanto, em 2005 passou por nova reformulação, continuando com sua estrutura, todavia, novos assuntos foram incluídos devido à evolução na tecnologia. Nesta versão 3.0, foi criada uma parte específica sobre códigos maliciosos, ampliada a parte sobre segurança de redes sem fio e incluídos tópicos sobre segurança em dispositivos móveis.

Novamente sofreu alterações a referida Cartilha em 2012, dando origem à versão 4.0, justificando-se tal modificação pelo uso

crescente da Internet e das redes sociais, impulsionado principalmente pela popularização dos dispositivos móveis e facilidades de conexão. Com isso, houve a necessidade de abordar novos conteúdos e agrupar os assuntos de maneira diferente, transformando-se em um livro totalmente ilustrado, com o objetivo de facilitar a leitura e torná-la mais agradável.

Essa Cartilha dispõe sobre os riscos relacionados à utilização dos *Cookies,* como por exemplo, o compartilhamento de informações e a exploração de vulnerabilidade, considerando que alguns programas guardam informações técnicas sobre o computador do usuário Identificam-se também como riscos a autenticação automática e a coleta de informações pessoais (CGL.BR, 2012, p. 40).

Não obstante a importância para prescrever direitos e deveres na utilização da internet, a Cartilha, não possui força normativa, surgindo a necessidade premente de normatização do uso dos ambientes virtuais, a fim de estabelecer regras e princípios para a proteção de novos direitos e, consequentemente proteger os dados dos usuários, coibindo eventuais abusos. Por esta razão, revela-se como bem vinda a aprovação da Lei 12.965/2014, denominada Marco Civil da Internet.

Foi também objeto de preocupação do Marco Civil da Internet a responsabilidade civil pelos danos causados por conteúdos gerados por terceiros, ao estabelecer que o provedor de conexão à internet não será responsabilizado por danos decorrentes de conteúdo gerado por terceiros (art. 18). O provedor somente poderá ser responsabilizado, se após ordem judicial específica, não tomar as providências de tornar indisponível o conteúdo apontado como infringente (art. 19).

Nesse contexto, também fora objeto de discussão se a responsabilidade civil dos provedores seria objetiva, com fundamento na teoria do risco, entretanto, se constatou que a responsabilidade objetiva dos provedores de serviços de internet, em qualquer situação, se apresenta como incorreta e, porque não

dizer injusta, considerando inclusive, que nenhum país adota tal modalidade.

A ausência total de responsabilidade não se afigura de igual modo como adequada, por estimular comportamentos omissos e total descaso dos provedores. Por esta razão, o Marco Civil pretendeu imputar responsabilidade somente quando houver descumprimento de ordem judicial.

Assim, conclui-se que, quando ocorrer a hipótese de postagens com conteúdos gerados por terceiros, o ofendido terá que acionar em primeiro lugar, o autor do conteúdo e não o provedor de conexão, sendo este responsabilizado somente se não cumprir ordem judicial de retirada do conteúdo da *web*. De qualquer sorte, o referido regramento pretende tutelar a liberdade de expressão, ao não permitir que em qualquer hipótese o provedor seja obrigado a retirar conteúdos da internet, apenas por mero capricho do suposto ofendido.

De fato, a Lei n. 12.965/2014, denominada de Marco Civil da Internet revela-se como avanço, fixando um marco histórico e jurídico de utilização da *web* no Brasil. Aplica-se a todas as situações em que esteja em perigo a privacidade do usuário, mas também tendo sido respeitada a liberdade de expressão das pessoas como direito igualmente integrante da personalidade humana. No entanto, verifica-se que, mesmo com o advento desta lei, não se conseguiu resolver o problema da proteção dos dados pessoais.

4.4 Lei de proteção de dados pessoais no Brasil

Como já se teve oportunidade de mencionar neste trabalho, o Brasil até 2018 era o único país da América Latina[5] que não

[5] O Chile possui, desde 1999, legislação nesta matéria – Lei 19.628/99. Disponível em http://www.sernac.cl/leyes/comppendio/docs_compendio/ley19628.pdf. Acesso em: 15 de jun. 2014. Na argentina, a Lei 25.326/2000. Disponível em http://www.jus.gob.ar/datos personales.aspx. Acesso em: 15 de jun. de 2014. No México a legislação de proteção de dados pessoais surgiu em 2010

dispunha de uma legislação específica de proteção a dados pessoais, mas tão somente normatizações genéricas que, por sua própria natureza, não conseguiram tutelar de forma efetiva os direitos relacionados a dados pessoais, como a privacidade e a intimidade[6].

Dessa forma, percebe-se como o Brasil passou grande tempo sem a proteção no que se refere a dados pessoais, muito embora encontram-se legislações que tratam superficialmente do tema, mas não da forma que a matéria merece. Tramitavam na Câmara dos Deputados basicamente dois projetos de leis sobre a referida matéria. O PL 4060/12, de autoria do Deputado Milton Monti, que passou alguns anos parado. E o PL 5276/16 de autoria do Poder Executivo, por intermédio do Ministério da Justiça.

O PL 4.060/12 foi dividido em três capítulos, que agrupam vinte e cinco artigos, dos quais o primeiro, que trata de disposições gerais, enuncia os princípios norteadores, estabelece as definições legais e delimita o escopo de abrangência, que é o tratamento de dados pessoais realizado em território nacional, ainda que o banco de dados esteja armazenado em território estrangeiro.

O segundo Capítulo dispõe sobre os requisitos para tratamento dos dados pessoais, exigindo que os responsáveis pelo tratamento dos dados adotem medidas tecnológicas, proporcionais ao estado da tecnologia, que minimizem os riscos de acesso não autorizado ou de perda dos dados dos titulares. Os dados pessoais poderão ser processados respeitada a lealdade e a boa fé e observado o legítimo interesse dos titulares.

O terceiro e último Capítulo trata do direito dos titulares dos dados de requerer, a qualquer momento, o bloqueio do tratamento

---

– *Ley federal de Protección de Datos Personde los Particularesales em Posesión de los particulares.* Disponível em: http://www.ifai.org.mx/. Acesso em 15 de jun. de 2014.

[6] A Lei de proteção de dados chilena tem características especificas que a difere das demais legislações dos países vizinhos. Foi fortemente influenciada pela lei espanhola. Destacando-se a ausência de uma autoridade de garantia, pois cabe ao interessado o recurso à justiça ordinária, bem como identifica-se ainda, uma ausência de responsabilidade objetiva do gestor dos dados.

de suas informações pessoais, assim como seu amplo acesso à política de privacidade dos responsáveis pelo tratamento.

O Projeto de Lei 5.276/16, de autoria do Poder Executivo foi apenso ao Projeto de Lei principal que trata do tema de maneira mais extensiva. Possui 56 artigos, divididos em nove capítulos. A proposta foi fruto da Resolução da ONU, de 25 de novembro de 2013, sobre "Direito à Privacidade na Era Digital".

O objetivo central do Projeto de Lei 5.276/16 é assegurar ao cidadão o controle e a titularidade sobre suas próprias informações, como forma de garantir a tutela do direito à privacidade informacional, bem como ao direito à intimidade. Note-se que, com os avanços na tecnologia de informação e comunicação, torna-se cada vez mais comum a obtenção e utilização de informações, sem o conhecimento do seu titular.

Em uma sociedade da informação como a que se vive atualmente, em que os dados representam um bem valioso, revelando-se como representação da própria personalidade do indivíduo, um regramento específico terá como principal beneficiário o cidadão, como titular dos dados pessoais, devendo ser considerado parte mais frágil nas relações que envolvem grandes organizações empresariais e o próprio Estado.

Com o advento de uma regulação de proteção de dados, o indivíduo passa a ter maior segurança no que diz respeito ao tratamento adequado de tais informações, que compõem sua privacidade e intimidade.

Merece destaque a natureza principiológica dada ao Projeto de Lei n. 5.276/16 (art. 6º), com influência das Diretivas da União Europeia, sobretudo da Diretiva 95/46/CE. A proposta de lei trazia como base a previsão de dez princípios para a proteção de dados pessoais, tais como: finalidade, necessidade, livre acesso, proporcionalidade, qualidade de dados, transparência, segurança física e lógica, boa-fé objetiva, responsabilidade e princípio da prevenção.

O projeto – PL 5276/16 foi resultado de um amplo debate público promovido on-line pelo Ministério da Justiça, que teve duração de quase seis meses, recebendo mais de 50 mil visitas e obtendo mais de 1.100 contribuições. No entanto, tal projeto de lei foi apenso ao PL 4060/12, que posteriormente transformou-se na Lei 13.709/18.

O art. 2º da novel legislação previu os fundamentos da disciplina da proteção de dados pessoais, tais como: I-respeito à privacidade; II- a autodeterminação informativa; III- a liberdade de expressão, de informação, de comunicação e de opinião; IV- a inviolabilidade da intimidade, da honra e da imagem; V – o desenvolvimento econômico e tecnológico e a inovação; VI – a livre iniciativa, a livre concorrência e a defesa do consumidor e; VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Logo no art. 5º, o legislador pretendeu estabelecer alguns conceitos-chave para uma melhor compreensão do texto em análise, como por exemplo, o de dado pessoal, tratamento, bancos de dados, dados sensíveis e outros, como se veem:

Art. 5º Para os fins da presente lei, entende-se como:

I – dado pessoal: qualquer informação relativa a uma pessoa identificada ou identificável, direta ou indiretamente, incluindo todo endereço ou número de identificação de um terminal utilizado para conexão a uma rede de computadores.

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios

técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

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

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII - encarregado: pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional;

IX - agentes de tratamento: o controlador e o operador;

X - tratamento: toda operação realizada com dados pessoais, como as que se

XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

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

XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;

XIX - autoridade nacional: órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento desta Lei.

Entende-se que o conceito de dados sensíveis se apresenta como um dos mais importantes para a discussão desta temática, considerando o efeito devastador que o tratamento e utilização de tais dados podem trazer para o seu titular, sobretudo quando utilizados para fins discriminatórios. Como se pode perceber, as

grandes organizações têm se utilizado de bancos de dados cadastrais para construir verdadeiros perfis das pessoas, sem qualquer critério de classificação e, com isso decidir com quem desejam contratar.

Sem contar no âmbito trabalhista, em que os empregadores buscam a todo custo, devassar toda a vida de um potencial colaborador, com o objetivo de reduzir as chances de "erro" na escolha. Todavia, essa intromissão na vida privada das pessoas só seria possível se fosse com o seu consentimento, que na maioria das vezes, nem elas mesmas têm o conhecimento de tal fato.

Essa invasão na privacidade informacional dos indivíduos traz efeitos absolutamente maléficos à sua personalidade, considerando que se trata de informações que só dizem respeito à própria pessoa, ao âmbito mais reservado possível, como os dados referentes à convicções religiosas, filosóficas, políticas, bem como orientações sexuais e aquelas atinentes à saúde da pessoa.

Ainda no que concerne ao inciso II do art. 5º, o legislador, ao conceituar dados sensíveis, mencionou os "dados referentes à saúde e à vida sexual", todavia, parece mais adequado utilizar a expressão "orientação sexual", pois a primeira pode ser interpretada restritamente, considerando ainda recentes eventos envolvendo preconceito oriundo de orientação sexual. Portanto, deve-se tomar o devido cuidado em dar proteção a este tipo de informação.

A legislação ora em discussão estabelece que nenhuma pessoa será obrigada a fornecer dados sensíveis, ficando proibida a formação de bancos de dados que contenham informações que, direta ou indiretamente, revelem dados sensíveis, salvo disposição legal expressa, respeitados os direitos de personalidade, especialmente a garantia à não discriminação, conforme o c*aput d*os art. 11, § 2º.

No entanto, a referida normatização prevê algumas hipóteses em que serão admitidos o tratamento de dados sensíveis, como por exemplo, se o titular houver dado o seu consentimento

livre, informado e por escrito, sempre que este tratamento for indispensável para o legítimo exercício das atribuições legais ou estatutárias de seus responsáveis (art. 11).

Nesse sentido, pode-se afirmar que a legislação de proteção de dados pessoais, recém aprovada e sancionada – Lei 13.709/18 busca resgatar direitos valiosos à personalidade, como a privacidade informacional que, não obstante seja tutelada de forma genérica pela nossa Lei Maior, necessita de uma atenção especial por parte do legislador infraconstitucional, considerando os avanços na tecnologia de informação e comunicação ocorridas nos últimos anos.

Atualmente se fala, a exemplo da legislação chilena de proteção de dados pessoais[7], em um termo inovador que caracteriza dados sensíveis, qual seja: "hábitos pessoais". Tal expressão envolve os gostos das pessoas, suas preferências, desejos e prováveis intenções para o consumo, ou seja, todas as informações necessárias para a tomada de decisões. Tal fato se justifica por conta do momento atual denominado "era da informação", consagrando a informação propriamente dita como instrumento de grande valia para o estudo do comportamento das pessoas e do mercado. Entretanto, a legislação brasileira não atentou para esta categoria de dados sensíveis, preferindo um conceito um tanto mais genérico.

4.4.1 O consentimento no tratamento de dados pessoais

Verifica-se que a legislação ora analisada teve uma preocupação especial com o consentimento, enfocando o poder do indivíduo de exercer um controle absoluto das informações que lhe dizem respeito. Cabe apenas ao indivíduo, o direito de autorizar a utilização dos seus dados pessoais. A esse respeito, os projetos de lei utilizam as palavras-chave: consentimento e autorização.

[7] Lei nº 19.628/99 sobre *protección de la vida privada o protección de datos de carácter personal*. Publicada en el Diario Oficial de 28 de agosto de 1999. Disponível em: http://www.sernac.cl/leyes/compendio/docs_compendio/ley19628.pdf. Acesso em: 01 de jul.2014.

O consentimento para o tratamento de dados pessoais é um dos pontos mais sensíveis desta temática (DONEDA, 2006, p. 371). Por intermédio dele, o direito civil tem a oportunidade de estruturar, a partir da autonomia da vontade, uma disciplina capaz de harmonizar os efeitos deste consentimento com os demais interesses em jogo. Enquanto expressão da autonomia da vontade, o consentimento deve ser interpretado como uma manifestação da escolha individual. As possibilidades de escolhas do indivíduo têm reflexos diretos nos direitos da personalidade, considerando que vários destes direitos dependem de certa forma da autonomia da vontade.

O art. 7º da Lei 13.709/18 trata dos requisitos para o tratamento de dados pessoais, que somente pode ocorrer após o consentimento livre, expresso, e informado do titular, podendo ser dado por escrito ou por outro meio que o certifique.

As pessoas que realizam o tratamento de dados pessoais têm o dever de informar de maneira clara e explícita ao titular dos dados: a finalidade para a qual os seus dados estão sendo coletados e de que forma serão tratados; a identidade e o domicilio do responsável pelo tratamento; a natureza obrigatória ou facultativa do fornecimento de dados; os sujeitos para os quais os dados podem ser comunicados e os seus direitos, em particular a possibilidade de se negar a fornecer tais dados e sobre seu direito de acesso e retificação dos mesmos.

Em alguns casos, o consentimento poderá ser dispensado, como por exemplo, quando for necessário à execução de obrigações derivadas de um contrato no qual é parte o titular, assim como também para execução de procedimentos pré-contratuais requeridos por este, ou para o cumprimento de uma obrigação legal por parte do responsável.

O consentimento pode ser dispensado, ainda, quando se estiver diante de tratamento de dados para fins estatísticos. Nessa hipótese especifica, deve-se tomar cuidado, pois atualmente há

pesquisas comportamentais tendo por base dados coletados dos indivíduos com informações dissociadas.

Essa metodologia utiliza dados coletados durante a utilização de s*ites* pelo usuário, por meio dos chamados *Cookies*, permitindo traçar perfis de grupos específicos, que podem levar ao cruzamento de dados. Essa análise estatística do comportamento virtual das pessoas pode levar a influenciar a coletividade e os hábitos dos usuários, tais como: o horário em que acessam determinado s*ite,* as páginas mais acessadas, os serviços mais utilizados e outros dados que podem ser relevantes quando não dissociados.

Por outro lado, o titular dos dados pessoais poderá se recusar a revelá-los, exercendo assim, o seu poder de autodeterminação, o que na maioria das vezes o faria ficar de fora daquela relação negocial, impossibilitando-o do acesso a determinados bens e serviços. Por esta razão, Rodotá (1973, p. 45-51), o considera um "mito", pois a sua utilização como instrumento para a tutela dos dados pessoais deve ser verificada a partir de sua concreta aplicação.

Tome-se como exemplo, uma pessoa que pretende adquirir um bem, financiado por instituição financeira, deverá preencher um cadastro. No entanto, não lhe convém responder a certas questões, por envolver dados considerados sensíveis. Tal circunstância faz com que a instituição financeira não aceite contratar, por faltar informações pessoais, consideradas relevantes para as organizações empresariais. Na verdade, o indivíduo não tem muita opção, ou ele aceita a conceder todas as informações necessárias para a celebração do contrato ou não poderá adquirir o bem.

Vê-se que aqui não se está tratando do consentimento negocial, mas sim de consentimento para tratamento de dados pessoais, que é bem mais especifico do que aquele concedido para a celebração de contratos, por exemplo. Nesse sentido, Doneda adverte que:

> Os parâmetros a serem levados em consideração para determinar o perfil deste consentimento, no entanto, não são os mesmos que embasam a atuação da autonomia privada nos mecanismos negociais tradicionais, e devem levar em conta fatores que, ao fim, este consentimento um tanto particular. Ao traçar este perfil, uma advertência previa seria resistir à tentação de utilizar mecanismos negociais em suas vestes tradicionais sem que se verifique a sua adequação. Isto porque os problemas derivados de uma transposição rasa do consentimento negocial para o consentimento ao tratamento de dados pessoais estão presentes em toda a crítica ao "mito do consentimento". (DONEDA, 2006, p. 376-377)

Assim, entende-se que não se revela adequado caracterizar o consentimento como sendo de natureza negocial. Se assim o fosse, dificultaria ou mesmo impossibilitaria a tutela dos dados pessoais, como atributo da personalidade. O consentimento para tratamento de dados pessoais está diretamente vinculado a elementos da própria personalidade, todavia não dispõe destes elementos, já que assume a natureza de um ato unilateral, quando concede autorização para tratamento de dados pessoais.

Verifica-se, portanto, que o consentimento poderá assumir o papel de instrumento da autodeterminação, sendo um aspecto da tutela da personalidade, bem como poderá desnudar-se em fator de legitimação para que os dados sejam utilizados por terceiros. Todavia, não se pode interpretar esta última hipótese como de natureza negocial, mesmo que possa parecer que o indivíduo que autoriza o uso de dados por terceiros, o faria em troca de alguma vantagem, até porque acarretaria a utilização de esquemas proprietários para o tratamento destes dados.

A concepção da natureza não negocial do consentimento para o tratamento de dados pessoais, traz a conclusão de que teria natureza de ato jurídico unilateral, considerando que o seu consentimento não tem efeitos vinculantes de natureza obrigacional, ou seja, o indivíduo pode pretender revogar o seu ato após ter autorizado, não representando assim, inadimplemento.

Assim, questiona-se: quem assumiria o risco de uma possível revogação do consentimento para tratamento de dados? Tratando-se de ato unilateral, todos os riscos decorrentes da revogação correrão por conta daquele que recebeu a autorização para tratamento de dados. No entanto, deve-se tomar cuidado para que esta revogação não se revele abusiva, podendo ensejar, inclusive, reparação de dados. De qualquer modo, não se pode colocar nenhum tipo de óbice para a possibilidade de revogação do consentimento, direito este previsto no art. 8, §5º da Lei 13.709/18.

Nesse contexto, Pinto (2002, p. 62) cita como exemplo de abuso, uma pessoa que após ter concedido autorização e recebido uma contrapartida, imediatamente revoga o consentimento para celebrar contrato mais vantajoso, o que nesse caso, só poderia ser combatido de *iuri condito* através de recurso a mecanismos gerais como o do abuso de direito ou do *venire contra factum proprium*.

Após dado o consentimento para tratamento de dados pessoais, o seu titular tem o direito de obter do responsável a confirmação da existência de dados pessoais que lhe dizem respeito, bem como terá acesso aos dados em si, inclusive por meio de *habeas data*.

As informações solicitadas poderão ser fornecidas por meio eletrônico, seguro e idôneo; ou sob a forma impressa, podendo ser cobrado valor necessário para cobrir os custos.

O titular dos dados pessoais poderá solicitar revisão de decisões tomadas com base em tratamento de dados automatizados que afetem seus interesses, inclusive decisões que destonadas a definir seu perfil ou avaliar aspectos da sua personalidade (art. 20)

O titular dos dados pessoais poderá ainda, conforme o art. 18, §2º da Lei 13.709/18, opor-se ao tratamento de seus dados, com fundamento em uma das hipóteses de dispensa de consentimento. Trata-se de direito de oposição, como corolário do direito ao consentimento.

Percebe-se que o legislador também se preocupou com a segurança dos dados pessoais a ser tratados ou manipulados. Estabelece que o tratamento de dados será feito de modo a reduzir ao mínimo o risco de sua destruição ou perda, bem como o risco de acesso não autorizado ou de tratamento não permitido pelo titular. Também foi objeto de preocupação o desvio de finalidade para a qual as informações foram coletadas.

Pode-se identificar como medida de segurança preventiva dos dados, a auto-regulamentação. Consiste no estabelecimento de regras provindas de fontes não estatais, como os códigos de condutas adotados por associações ou organizações empresariais. Todavia, não se revela como alternativa satisfatória, tendo em vista que suas regras são não vinculantes, posto emanadas fora do âmbito estatal. Sem falar que pode ocorrer conflito de interesses, já que são emanadas por entidades que detêm interesse na exploração do tratamento de dados pessoais.

Fala-se ainda em métodos baseados na própria tecnologia, onde são criados para atuar na arquitetura da privacidade, impossibilitando, limitando ou mesmo facilitando uma determinada ação que englobe o tratamento de dados pessoais, como por exemplo, aquelas que garantem o anonimato (DONEDA, 2006, p. 368).

A tecnologia como meio de tutela dos dados pessoais, também não se revela satisfatória, muito embora seja considerada por muitos como importante, não só em matérias que envolvem a privacidade, mas também naquelas ligadas à arquitetura da comunicação. A sua aplicação não pode ser compreendida isoladamente, podendo ser um importante instrumento auxiliar de garantia da tutela dos dados pessoais.

Ainda como medida de segurança dos dados pessoais, a referida legislação de proteção de dados prevê no art. 48 que o controlador deverá comunicar ao órgão competente a ocorrência de qualquer incidente de segurança que possa acarretar risco ou prejuízo aos seus titulares.

Outra questão que merece especial atenção é aquela referente à comunicação e interconexão dos dados pessoais. Com a evolução nas tecnologias de informação e comunicação, esta prática passou a ser corriqueira nas grandes organizações empresariais. Atualmente, revela-se muito comum, empresas que disponibilizam ou até comercializam dados pessoais com o absoluto desconhecimento dos seus titulares.

Destaca-se que a comunicação ou interconexão dos dados pessoais só é possível com a permissão do seu titular, sendo tal consentimento revogável a qualquer tempo. Note-se a importância que foi dada ao consentimento pelo legislador, considerando que a proteção de dados pessoais está diretamente ligada à personalidade, por intermédio da privacidade e intimidade das pessoas.

No entanto, entende-se que na prática não se revela fácil o cumprimento do requisito do consentimento para quaisquer formas de tratamento de dados pessoais, diante dos recursos que a tecnologia coloca à disposição, principalmente das grandes organizações. Por exemplo, o indivíduo disponibiliza seus dados pessoais ao preencher cadastro em uma empresa privada. Meses depois, uma instituição financeira, de posse do cadastro desta pessoa, entra em contato para oferecer empréstimos e cartões de crédito, por ter tido acesso a estas informações, que contribuíram para a constituição de um dado perfil de interesse daquela empresa.

Em algumas situações, a comunicação ou transmissão dos dados pessoais para terceiros se faz de forma comercializada, o que demonstra uma grande ameaça aos direitos da personalidade do indivíduo. Todavia, há quem entenda, como Pinto (2002, p. 52) que a comercialização de dados pessoais é plenamente admissível, não podendo se fazer analogia com os casos de comercialização de órgãos ou parte do corpo humano. O referido autor defende ainda, um reconhecimento de uma dimensão patrimonial em muitos direitos da personalidade.

Com todo o respeito ao mencionado autor, entende-se que não se pode fazer qualquer analogia entre a comercialização de

informações pessoais com a comercialização de órgãos. Trata-se de direitos da personalidade diferentes. No primeiro caso, está em jogo a privacidade informacional e, no segundo, direito à integridade física. No entanto, não se pode vislumbrar como adequada a tese que defende a comercialização de dados pessoais, considerando que se assim fosse estar-se-ia desqualificando a autonomia da vontade do titular dos dados, sem contar que estão em jogo direitos inerentes à personalidade humana, indisponíveis.

Entende-se ainda que a possibilidade de "comercialização de dados pessoais" só se afiguraria como possível, havendo previsão expressa na lei de proteção de dados pessoais, o que não ocorreu na legislação em análise, nem tão pouco nas legislações que serviram de base para elaboração de tal proposta de lei. Somente a lei poderia restringir direitos relacionados a proteção de dados pessoais, como faz o Código Civil brasileiro, quando possibilita, excepcionalmente, o uso da imagem da pessoa, quando autorizada por ela ou quando necessária à administração da justiça, conforme o art. 21.

Ao término do tratamento, os dados pessoais deverão ser cancelados quando deixarem de ser necessários ou pertinentes à finalidade pela qual foram coletados. Todavia, o legislador previu a possibilidade de conservar os dados nas hipóteses previstas no art. 16.

A legislação em análise trata da matéria tanto no setor público como no setor privado. Como o objeto deste trabalho é a proteção de dados pessoais por agentes privados, as próximas considerações serão direcionadas a este setor.

O responsável pelo tratamento de dados – controlador e operador terão como funções: atuar como correspondente imediato do órgão competente; receber reclamações e comunicações dos titulares; orientar os demais funcionários a respeito das práticas a ser tomadas em relação à proteção de dados pessoais e; manter uma relação dos tratamentos de dados pessoais realizados pela empresa que sejam acessíveis aos seus titulares que o requisitarem.

4.4.2 A Autoridade Nacional de proteção de dados pessoais

Pela análise do projeto de lei, verifica-se que a Autoridade Nacional foi diversas vezes citada, mas importa saber, o que mesmo significa esta autoridade? Quais as suas funções e o seu papel na proteção de dados pessoais? Do ponto de vista prático, a referida autoridade contribuirá de forma positiva para proteção de dados pessoais?

Nos dias atuais, a vida das pessoas envolve uma troca continua de informações, com um grande fluxo de dados, com isso, se atribui importância especial à proteção de dados pessoais. Esta evolução é bastante visível em outros países, sobretudo naqueles que integram a União Europeia. A legislação sobre proteção de dados pessoais fixa regras sobre as modalidades de tratamento, concretizando-se em poderes de intervenção.

Estes poderes de controle e intervenção não devem mais ser atribuídos somente aos interessados diretos, isto porque como ensina Rodotá (2008, p. 199), devem ser confiados também a uma autoridade independente, envolvendo uma responsabilidade pública específica.

A legislação italiana, mais especificamente o Código em matéria de tratamento de dados pessoais – Decreto Legislativo nº 196, de 30 de junho de 2003, previu expressamente a figura do Garante, no seu art. 153 e 154. Dispôs inicialmente que, o Garante atuará com plena autonomia e independência de juízo e de valoração. Formado por um órgão colegiado, constituído por quatro membros, sendo dois eleitos pela Câmara dos Deputados e dois pelo Senado da República com voto limitado. Os membros deverão ser escolhidos entre pessoas com notória competência nas matérias do direito ou da informática[8].

[8] O Art. 153 do Código em matéria de Proteção de Dados Pessoais estabelece que: "1. Il Garante opera in piena autonomia e con indipendenza de giuduzio e di valutazione. 2. Il Garante e' organo collegiale costituito de quatro componenti, eletti due dalla Camera dei deputatu e due dal Senato dellla Repubblica com voto limitadto. I componenti sono scelti tra persone che assicurano indipendenza e che sono esperti

Vê-se que a legislação italiana se preocupou logo em fixar regras para a nomeação dos membros que comporão o órgão colegiado, da forma mais democrática possível, demonstrando-se dessa forma, a caraterística basilar de um órgão independente e autônomo, sem subordinação a nenhum dos poderes.

Com foi visto acima, o recurso a uma autoridade administrativa se justifica pelo fato de que não se pode mais deixar apenas nas mãos do indivíduo esta tarefa, considerando que na maioria das vezes o titular dos dados não tem ao menos o conhecimento de que suas informações pessoais estão em poder de determinada pessoa.

A ideia de uma Autoridade de Garantia partiu desde o advento da Diretiva 95/46/CE, em que impôs aos países-membros da União Europeia, a obrigatoriedade de sua instituição, passando a ser uma caraterística marcante do modelo europeu. No entanto, posteriormente foi adotado por outros países, que não integram a União Europeia, como Argentina, Austrália, Canadá, Japão.

Nos Estados Unidos, pode-se citar a *Federal Trade Comission* – FTC, que, embora não seja um órgão equiparado à Autoridade de Garantia, recebeu a incumbência de fiscalizar a utilização de dados pessoais, que por ter bem cumprido tal encargo, lhe rendeu o título de uma *authority* de fato por alguns estudiosos (DONEDA, 2006, p. 387).

No modelo norte-americano, a previsão de uma Autoridade de Garantia é perfeitamente dispensável, já que a tutela naquele país se concentra na via judicial; ao contrário do modelo europeu, que considera a autoridade administrativa indispensável para a proteção dos dados pessoais.

Mesmo antes do advento da Diretiva 95/46/CE, a Carta dos Direitos Fundamentais da

---

di riconosciuta competennza dele materie del diritto o dell'informatica, garantindo la presenza di entramble le qualificazioni". Disponível em: http://www.parlamento.it/parlam/leggi/deleghe/03196dl.htm. Acesso em: 20/04/2014.

União Europeia, em 1980 já previa a existência de uma autoridade independente no seu art. 8°, 3 "O cumprimento destas regras fica sujeito à fiscalização por parte de uma autoridade independente".

O recurso à um órgão de fiscalização e controle, dotado de independência é uma prática bastante comum nos Estados democráticos. O ente estatal, não tendo mais condições de arcar com a responsabilidade pela fiscalização dos diversos serviços públicos postos à disposição do cidadão, bem como pela necessidade de se regular determinadas áreas do mercado, cria órgãos de controle e fiscalização.

Pode-se citar como exemplo no Brasil, as chamadas agências reguladoras[9], tais como: Agência Nacional de Telecomunicações – ANATEL; Agência Nacional de Petróleo – ANP; Agência Nacional de Energia Elétrica – ANEEL; Agência Nacional de Saúde Complementar – ANS; Agência Nacional de Vigilância Sanitária – ANVISA; Agência Nacional de Aviação Civil – ANAC, dentre outras.

Não se pretende afirmar que o órgão que compõe a Autoridade de Garantia seja uma agência reguladora, mas tão somente demonstrar as semelhanças entre ambas, já que têm funções de órgão controlador e fiscalizador[10].

---

[9] As agências reguladoras surgiram quando da instituição das autarquias de controle, consideradas autarquias sob regime especial, tendo como prerrogativas: a) poder normativo técnico; b) autonomia decisória; c) independência administrativa e; autonomia econômico-financeira. O poder normativo indica que estes órgãos recebem a delegação de editar normas técnicas de caráter geral, retratando um poder regulamentar mais amplo. Já a autonomia decisória significa que os conflitos administrativos se desencadeiam e se dirimem através dos próprios órgãos da autarquia. A independência administrativa refere-se ao fato de que alguns dos seus dirigentes têm investidura a termo, sendo nomeados para prazo determinado, como por exemplo, um cargo em comissão, não obstante a investidura por prazo certo. Por fim, a autonomia econômico-financeira demonstra que estas autarquias têm recursos próprios, recebendo dotações orçamentárias para gestão por seus órgãos. (CARVALHO FILHO, 2009, p. 454-457).

[10] Em Parecer elaborado pelo escritório de advocacia Patrícia Peck Pinheiro Advogados – PPP, localizado na cidade de São Paulo- SP, como contribuição para redação do Anteprojeto de Lei de proteção de dados pessoais, destacou que o Brasil optou por um modelo arrojado, adotando um sistema que possui componente legislativo delineado os dogmas e a conduta esperada daqueles que praticarem o tratamento de dados e, que por seu turno, criará um conselho controlador e fiscalizador, similar a de uma Agência Reguladora, como o objetivo de resolução de conflitos,

Dessa forma, estes órgãos podem ser definidos como sendo entes públicos, dotados de independência em relação aos demais poderes do Estado, assim como também dotados de autonomia administrativa e financeira, com a função precípua de controlar e fiscalizar determinadas áreas do mercado.

No entanto, na Lei 13.709/18, a parte que tratava da Agência Nacional de proteção de Dados Pessoais foi vetada pelo Presidente Michel Temer. O governo entendeu que haveria uma inconstitucionalidade na criação de tal autoridade. O Presidente Michel Temer sinalizou que tal problema poderia ser solucionado por um outro projeto de lei, ou mesmo por intermédio de uma Medida Provisória.

A proposta é que tal autoridade seja independente, com orçamento próprio e capaz de fiscalizar, impor multas, dialogar com empresários de diferentes setores e estabelecer diretrizes para efetiva proteção dos dados pessoais. É importante mencionar que a criação de uma autoridade nacional de proteção de dados pessoais é indispensável para a concretização dos direitos previstos nessa legislação.

Nesse sentido, convém fazer distinção entre autoridade de regulação e autoridade de garantia. A primeira tem competência vinculada a determinado serviço público, com funções similares da própria administração pública. A autoridade de garantia teria a função de ponderar situações subjetivas previstas na Constituição, bem como operar um balanceamento dos direitos em questão, sem estarem vinculadas ao interesse público administrativo (LAZZARA, 2001, p. 80).

Dessa forma, corre-se o risco de o legislador brasileiro confundir os dois tipos de autoridades e transformar a denominada Autoridade de Garantia no Brasil em uma agência reguladora,

---

impasses e aplicação penalidades sem a necessidade de se recorrer ao judiciário. (PINHEIRO, Patrícia Peck. Disponível em: http://www.culturadigital/dadospessoais. Acesso em: 01 de jul. 2014).

como aquelas que já existem, mas que na prática não se mostram eficientes e satisfatórias para o cidadão.

Por esta razão, defende-se nesta tese, que o legislador brasileiro fixe desde logo a forma de criação deste órgão, bem como os membros que o integrarão, a exemplo do que fez a legislação italiana, que de modo mais democrático, decidiu que os membros fossem eleitos pela Câmara dos Deputados e Senado Federal, com mandato fixo, tornando legítimo o papel dos membros que irão compor a Autoridade de Garantia independente.

Nesse contexto, está tramitando na Comissão de Constituição e Justiça – CCJ do Senado Federal, o Projeto de Lei n. 464/2007, que pretende modificar as regras para indicação de diretores de agências reguladoras, exigindo dentre outros requisitos, experiência profissional de, no mínimo dez anos no setor objeto de regulação, podendo ser no setor público ou privado, exigindo ainda, formação acadêmica compatível com o cargo e nível acadêmico médio dos profissionais do setor que gozem de notório saber.

Justifica-se tal modificação, por ter a Lei n. 9.986/2000, que trata da gestão de recursos humanos das agências reguladoras, estabelecido requisitos um tanto genéricos para a indicação de seus diretores, demonstrado assim, maior discricionariedade por parte do chefe do poder executivo no momento da nomeação destes membros.

É importante frisar que uma das características basilares da Autoridade de Garantia é a sua independência, devendo afastar o máximo possível a possibilidade de ingerência ou subordinação dos poderes estatais constituídos. Por esta razão, é indispensável a criação de mecanismos que resguardem tal perfil, no momento da nomeação de seus membros, limitando a discricionariedade de sua escolha, com requisitos mais objetivos.

Não é demais lembrar que a forma de nomeação dos dirigentes das agências reguladoras obedece à mesma modalidade de indicação dos Ministros do Supremo Tribunal Federal que, não

obstante seja integrado por membros de notório saber jurídico e reputação ilibada, são nomeados pelo chefe do poder executivo, o que faz com que muitos autores não o considere uma verdadeira Corte Constitucional nos moldes europeus[11].

A constituição deste órgão que atuará como Autoridade de Garantia é de extrema importância para a efetiva proteção dos dados pessoais, como direito integrante da personalidade humana. Por esta razão merece do legislador uma atenção especial.

Resta demonstrado que o exercício da autodeterminação informativa apenas pela atuação do indivíduo se mostra ineficaz, considerando a desproporção entre os seus interesses e a existência de organizações encarregadas na coleta e tratamento de dados pessoais, destinadas a excluí-lo de certas relações, caso não forneça os dados solicitados.

O que se defende é que a tutela dos dados pessoais seja efetiva, considerando-se o estágio atual da tecnologia, bem como a dimensão jurídica internacional desta temática, tendo como centro de preocupação do ordenamento jurídico a pessoa humana.

Das configurações possíveis para este órgão, Doneda (2006, p. 401) identifica basicamente três opções: a de um órgão independente da estrutura estatal, de perfil que genericamente associa-se a uma agência; a de conceder a atribuição destas responsabilidades ao próprio Ministério Público ou; a de uma estrutura a *Dirección Nacional de protección de Datos Personales* – DPDP, conforme analisado no tópico 4.2.1 deste trabalho.

Observa-se que o órgão de controle por ter como característica essencial a independência, não poderia jamais ser vinculado a qualquer um dos poderes. Pela própria natureza da tutela que se pretende efetivar, exige-se desta autoridade uma neutralidade em face das razões do próprio Estado. Sem contar que

[11] O Tribunal Constitucional Alemão compõe-se de juízes federais e de outros membros, sendo eleitos pela metade dos integrantes do Parlamento Federal e do Conselho Federal, respectivamente. (GODOY, Arnaldo Sampaio de Moraes. *Corte Constitucional alemã é formada pelo legislativo.* Disponível em: http://www.conjur.com.br. Acesso em 01 de jul. 2014).

o poder executivo possui grande interesse na coleta e processamento de dados pessoais, o que pode ocasionar certo conflito de interesses diante de caso concreto.

Na hipótese ventilada por Doneda (2006) em relação à concessão de tais atribuições ao Ministério Público, teoricamente poderia ser uma solução adequada, já que é um órgão dotado de independência e isenção, todavia, deve-se lembrar que a Constituição Federal não lhes outorgou esta atribuição, portanto, a p*riori, e*staria descartada tal possibilidade.

Parece que o mais razoável seria interpretar o perfil da Autoridade de Garantia nos moldes assemelhados de uma agência, no entanto, deve-se ter o devido cuidado para não transformá-lo em uma agência reguladora. Essa autoridade deve prezar ao máximo pela sua autonomia e independência, como forma de garantir a efetividade da proteção dos dados pessoais. Deve-se ainda, observar os impactos do ponto de vista econômico para o Estado.

A referida legislação prevê ainda sanções administrativas a ser imputadas em hipótese de infrações das normas previstas na lei, tais como: multa; bloqueio dos dados pessoais; dissociação dos dados pessoais; proibição do tratamento de dados pessoais; suspensão temporária de atividade e; proibição de funcionamento do banco de dados. Tais sanções serão aplicadas pela Autoridade de Garantia, podendo ser aplicadas cumulativamente, conforme o caso.

No entanto, causa preocupação que a parte mais importante da legislação de proteção de dados pessoais no Brasil tenha sido vetada pelo Presidente da República, o que leva a se presumir pela não efetivação desta lei, se não for criada a Autoridade Nacional de proteção de dados.

A autoridade Nacional deverá impor ainda, de oficio ou a pedido da parte, as medidas coercitivas que considere necessárias para reverter efeitos danosos que a conduta infratora tenha causado ou para evitar que esta se produza no futuro novamente, fixando ainda, multa diária por dia de descumprimento.

Vê-se mais uma vez, como é importante o papel e a função da Autoridade Nacional, em um sistema de proteção de dados pessoais. Pode-se afirmar que a sua presença é indispensável para se efetivar a proteção deste direito fundamental. Por esta razão, é premente a sua criação para tornar efetiva a Lei geral de proteção de dados pessoais no Brasil.

Dentre as atribuições acima citadas, chama-se atenção para duas delas: a primeira no que diz respeito a sua competência para editar normas e provimentos. Esta pode ser alvo de críticas no que concerne ao princípio da separação dos poderes, já que é um órgão independente da estrutura dos demais poderes estatais. Tem-se aí um problema de legitimação da Autoridade Independente, já que não estaria legitimado diretamente pelo povo, não obstante a sua importância institucional.

A segunda consideração seria em torno da imposição de que a Autoridade Nacional promova o conhecimento das normas que tratam desta matéria. Entende-se como indispensável o dever de informação a todas as pessoas em relação à proteção de dados pessoais, pois normalmente o indivíduo não tem noção dos riscos à sua privacidade quando da utilização de seus dados pessoais. Note-se que o dever de informação da autoridade é correlato ao direito à informação do seu titular.

Por fim, a referida legislação trata da possibilidade de os responsáveis pelo tratamento de dados pessoais, individualmente ou por meio de organizações de classe, formularem códigos de boas práticas, estabelecendo as condições de organização, regime de funcionamento, procedimentos aplicáveis, normas de segurança e demais formas de garantia para as pessoas, com respeito aos princípios e normas de proteção de dados. Os códigos de boas práticas deverão passar pelo crivo da Autoridade Nacional, que poderá não aprová-lo se estiverem em desacordo com as disposições legais e regulamentares sobre a matéria.

Destaca-se que a nova lei de proteção de dados no Brasil seguiu as orientações do Regulamento Geral de Proteção de Dados

da União Europeia, que entrou em vigor em 2018, muito embora tenha também servido como base a Directiva 95/46/CE, que por muitos anos foi considerada o principal instrumento da União Europeia em matéria de proteção de dados pessoais.

Constata-se, por fim, que a efetividade do direito à privacidade informacional depende, em certa medida, de uma ação positiva por parte do Estado, isto porque o poder público tem o dever de implementar medidas administrativas e legislativas, necessárias à concretização deste direito tão valioso da personalidade humana.

Conclusão

A proteção dos dados pessoais revelou-se como tema de grande importância, diante das inovações tecnológicas nas áreas da informação e comunicação ocorridas nas últimas décadas. Esta matéria está intimamente intrincada com a tutela da privacidade, que restou ameaçada pelo advento da denominada "sociedade da informação".

Buscou-se neste trabalho contribuir para a compreensão da necessidade de ampliação da noção de direito à privacidade, em face destas novas investidas tecnológicas, considerando o contexto social, econômico e político que aí se instaurou. Para tanto, formulou-se as seguintes conclusões:

1) A privacidade é um conceito que passou por várias fases de desenvolvimento e, com isso suscitou muita discussão doutrinária e jurisprudencial. Inicialmente, considerada como direito ao recato e ao isolamento, apresentava um caráter individualista, próprio da época.
2) A privacidade na era da informação assumiu a feição atual, passando a ser entendida como autodeterminação informativa. Revela-se como a faculdade de o indivíduo obstar a intromissão de estranhos na sua vida privada. Apresenta-se ainda, como uma prerrogativa de controlar as informações pessoais que lhe dizem respeito.
4) A possibilidade de limitação deste direito deve ser ressaltada por via do legislador constitucional ou infraconstitucional, bem como por intermédio do judiciário, quando evidencia hipótese de conflito entre

dois direitos da personalidade, como por exemplo, a privacidade e a liberdade de expressão. Deve-se preservar na medida do possível, o núcleo essencial deste direito, não se admitindo que a pessoa seja reduzida a objeto de informação.

5) O âmbito de proteção da privacidade revela-se elástico e variável, podendo ser modificado conforme o tempo, o lugar e o titular dessa garantia. Como exemplo, a privacidade dos artistas em geral é representada por um âmbito de proteção muito menos rígido, do que àquela de uma pessoa anônima. Ou seja, quanto maior for a amplitude da pessoa pública, menor será a possibilidade de obstar intromissões na sua vida privada.
6) A íntima cumplicidade entre a privacidade e a intimidade foi constatada nesse trabalho muito embora tenha sido objeto de grandes controvérsias na doutrina. Alguns entendem como expressões sinônimas; outros defendendo a diferença entre os dois termos.
7) A diferença entre ambas foi demonstrada e para isso utilizou-se a teoria alemã das esferas ou dos círculos concêntricos, desenvolvida por Hubman. Por essa teoria, fica evidenciado que a vida privada corresponde à esfera mais ampla, protegendo fatos da vida particular, nos quais não revelam aspectos muito reservados, mas tão somente situações que se deseja preservar do conhecimento de terceiros. Já a intimidade vincula-se à esfera mais interior do indivíduo, onde podem ser encontrados os fatos e informações mais sensíveis, como os seus pensamentos e crenças.
8) A relação entre privacidade e informação, diante dos avanços tecnológicos no mundo globalizado é muito próxima. Hoje, o que de fato interessa é a privacidade informacional, consubstanciada no direito do indivíduo ter o absoluto controle sobre os seus dados.

9) O controle por parte do cidadão revela-se de difícil implementação, tendo em vista a rapidez e a maleabilidade das informações. Observa-se a necessidade de se adotarem medidas legislativas acerca da proteção de dados, pois as normas existentes postas à disposição do cidadão não são suficientes e adequadas para uma efetiva tutela.
10) O Brasil até 2018 era o único país do Mercosul a não possuir legislação acerca desta matéria, o que demonstra a fragilidade do direito à privacidade informacional nos dias atuais, em face das novas investidas tecnológicas.
11) A Lei Geral de Proteção de Dados Pessoais no Brasil, analisada no último capítulo desta tese, revela a grande influência sofrida pela legislação europeia, sobretudo, o Regulamento Geral de Proteção de Dados na União Europeia, bem como a Diretiva 95/46/CE. No entanto, demonstrou-se a preocupação em se utilizar como exemplo uma normatização, que apesar de ser paradigmática no assunto, reflete a realidade de países que compõem a União Europeia. Ou seja, não revela a realidade de um país em desenvolvimento, com fortes desigualdades sociais e um histórico de corrupção como o Brasil.
12) A tutela da proteção dos dados exige também outros instrumentos, como os códigos de boas práticas e a autorregulação, muito embora sejam considerados insuficientes, diante da ação das novas tecnologias existente. Tais instrumentos devem ser conjugados com outros para permitir uma efetiva tutela.
13) O controle das informações passa pelo consentimento e autorização do seu titular, que, na maioria das vezes, não tem o conhecimento acerca da utilização dos seus dados por parte de empresas privadas.

14) O indivíduo sozinho não teria condições de efetivar tal tutela, necessitando da figura de um *Garante* ou autoridade independente para desempenhar o papel de fiscalizar e controlar o tratamento de dados pessoais. Essa autoridade seria representada por um órgão, independente dos demais poderes, com plena autonomia. No entanto, no que se refere à legislação de proteção de dados no Brasil, essa parte foi vetada, com a justificativa de que a Constituição Federal determina que a criação de despesas que onerem o orçamento só possa ser pelo Poder Executivo.
15) A composição do referido órgão deve ser feita da forma mais democrática possível, com eleição de seus membros, que deverão ter notório saber nas áreas diretamente afetadas. A autoridade de garantia deve ter plena autonomia e independência na sua função de zelar pela proteção dos dados pessoais. Ademais, o próprio poder público revela-se como um grande catalizador de informações, podendo assim, caracterizar conflito de interesses.
16) Por fim, a fragilidade do direito à privacidade nos dias atuais é clara, diante dos recursos utilizados para a coleta, armazenamento e tratamento de dados pessoais. Defende-se assim, a importância da regulamentação especifica desta matéria, com a imediata previsão da Autoridade Nacional para fiscalizar e concretizar os direitos previstos na novel legislação.

Referências

ALEXY, Robert. **Teoria dos direitos fundamentais**. Trad. Virgílio Afonso da Silva. São Paulo: Malheiros, 2008.

ALONSO, Felix Ruiz. Pessoa, intimidade e o direito à privacidade. In: MARTINS, Ives Gandra; PEREIRA JUNIOR, Antônio Jorge (coordenadores). **Direito à privacidade**. São Paulo: Centro de Extensão Universitária, 2005.

AMARAL, Francisco. **Direito civil**: introdução. Rio de Janeiro: Renovar, 2006

ANDERSON , David. The Failure of American Privacy Law. In: Protecting Privacy. MARKESINIS, Basil (Org.). Oxford: Oxford University Press, 1999.

ARENDT, Hannah. A condição humana. Rio de Janeiro: Forense, 1995

ASCENSÃO, José de Oliveira. **Direito Civil**: teoria geral: introdução, as pessoas, os bens. Coimbra: Coimbra, 1997.

_____. **Direito da Internet e da sociedade da informação**. Rio de Janeiro: Forense, 2002.

BARROSO, Luís Roberto. A viagem redonda: habeas data, direitos constitucionais e provas ilícitas. In: WAMBIER, Teresa Arruda Alvin (coord.). **Habeas Data.** São Paulo: RT, 1998, pp.202-221.

BENJAMIN, Antônio Hermann. **Código Brasileiro de Defesa do Consumidor comentado pelos autores do anteprojeto**. Rio de Janeiro: Forense, 1997.

BESSA, Leonardo Roscoe. **O consumidor e os limites dos bancos de dados de proteção de crédito**. São Paulo: Revista dos Tribunais, 2003.

BITTAR, Carlos Alberto. **Os direitos da personalidade**. 7. ed., revista e atualizada de acordo com o novo Código Civil. Rio de Janeiro: Forense Universitária, 2006.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília, DF, 1988.

_____. Lei n. 12.965, de 23 Abril de 2014. **Estabelece princípios, garantias, direitos e deveres para uso da internet no Brasil**. Brasília, DF, 2014.

_____. Lei nº 10.406, de 10 de janeiro de 2002. **Institui o Código Civil.** Brasília, DF, 2002.

_____. Lei 12.527, de 18 de novembro de 2011. **Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 06 de abril de 2014.

_____. Lei 9.507/97, de 12 de novembro de 1997. **Regula o direito de acesso a informações e disciplina o rito processual do *habeas data*.** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L9507.htm. Acesso em: 06 de abril de 2014. _____. Lei nº 9.986, de 18 de julho de 2000. **Dispõe sobre a gestão de recursos humanos das Agências Reguladoras e dá outras providências.** Brasília, DF, 2000.

_____. Lei n. 11.419, de 19 de dezembro de 2006. **Dispõe sobre a informatização do processo judicial;** altera a Lei nº 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências. Brasília, DF, 2006

_____. Lei n. 11.990, de 27 de julho de 2009. **Abre aos Orçamentos Fiscal e da Seguridade Social da União, em favor da Presidência da República e dos Ministérios dos Transportes e das Cidades, crédito suplementar no valor global de R$ 638.258.797,00, para reforço de dotações constantes da Lei Orçamentária vigente.** Brasília, DF, 2009.

_____. Lei n. 4.595, de 31 de dezembro de 1964. **Dispõe sobre a Política e as Instituições Monetárias, Bancárias e Creditícias, Cria o Conselho Monetário Nacional e dá outras providências**. Brasília, DF, 1964.

_____. Lei n. 8.078, de 11 de setembro de 1990. **Institui o Código de Defesa do Consumidor**. Brasília, DF, 1990.

_____. Projeto de Lei nº 464/2007. **Modifica as regras para indicação dos diretores das agências reguladoras.** Brasília, DF, 2007. Disponível em: http://www.senado.gov.br . Acesso em 23 de junho de 2014.

_____. Projeto de Lei nº 2.126/2011. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Brasília, DF, 2011. Disponível em: http://www.senado.gov.br . Acesso em 23 de junho de 2014.

_____. Lei nº 7.232/84. **Dispõe sobre a Politica Nacional de Informática, prevendo a estruturação e exploração dos bancos de dados**. Brasília, DF, 1984. Disponível em: http://senado.gov.br. Acesso em:30 de junho de 2014.

_____. Lei n. 9.296, de 24 de julho de 1996. **Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal**. Brasília, DF, 1996.

_____. Lei n. 12.106, de 2 de dezembro de 2009. **Cria, no âmbito do Conselho Nacional de Justiça, o Departamento de Monitoramento e Fiscalização do Sistema Carcerário e do Sistema de Execução de Medidas Socioeducativas e dá outras providências**. Brasília, DF, 2009.

_____. **Rede de Informações e Contrainformações do Regime Militar no Brasil**. Disponível em: http://www.arquivonacional.gov.br. Acesso em: 02 de jul. 2014.

_____. **Cartilha de Segurança para Internet. Centro de Estudos, Resposta e Tratamento de incidentes de segurança no Brasil – CERT**, 2012

_____. Supremo Tribunal Federal. **Reclamação n. 2.040/**DF. Relator Min. Neri da Silveira. Julgamento em 21/02/2002.

_____. Superior Tribunal de Justiça. **RESP nº 22.337/RS**. Recorrente: Clube de Diretores Lojistas de Passo Fundo-RS. Relator Min. Rui Rosado de Aguiar. Julgamento em 13/02/1995. Diário de Justiça em 20/03/1995. Disponível em: < http://stj.gov.br/SCON/jurisprudencia>. Acesso em 27 de jun. 2014.

_____. Superior Tribunal de Justiça. **Recurso Ordinário em Mandado de Segurança n. 15146/SC**. Relator Min. Luiz Fux. Julgamento em 18/03/2003.

_____. Ministério da Ciência de Tecnologia. **Livro Verde da Sociedade da informação no Brasil**. Brasília: Ministério da Ciência e Tecnologia, 2000.

BUENO, Cassio Scarpinella. Habeas Data. In: Fredie Didier Jr. (Org.). **Ações Constitucionais**. Salvador: Podivm, 2012.

BUTTARELLI, Giovanni. **Banchi Dati e tutela della riservatezza**. Milano: Giuffrè, 1997

CACHAPUZ, Maria Claudia. **Intimidade e vida privada no novo Código Civil Brasileiro** – uma leitura orientada no discurso jurídico. Porto Alegre: Sergio Antônio Fabris, 2006.

CAPELO DE SOUSA, Rabindranath Valentino Aleixo. **O direito geral de personalidade**. Coimbra: Coimbra, 2011.

CARVALHO FILHO, José dos Santos. **Manual de Direito Administrativo**. Rio de Janeiro: Lumem Juris, 2009.

CASTELLS, Manoel. **A galáxia da Internet**: Reflexões sobre a internet, os negócios e a sociedade. Trad. Maria Luiza Borges. Rio de Janeiro: Zahar, 2003.

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

CATALA, Pierre. Ebauche d'une théorie juidique de l'infomation. In: **Informatica e Diritto**, ano IX, jan-apr. 1983, p.15-31.

COSTA JUNIOR, Paulo José da. **O direito de estar só**: tutela penal da intimidade. São Paulo: Revista dos Tribunais, 2007.

CUPIS, Adriano de. **Os direitos da personalidade**. São Paulo: Quorum, 2008.

DANTAS, San Tiago. **Programa de Direito Civil**: Teoria Geral. Rio de Janeiro: Forense, 2001.

DINIZ, Maria Helena. **Curso de Direito Civil brasileiro**. São Paulo: Saraiva, 2004.

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

_____.Os direitos da personalidade no Código Civil de 2002. **Revista da Faculdade de Direito de Campos**, ano VI, n.06, Junho/2005.

_____. Um código para proteção de dados pessoais na Itália. In: **Revista Trimestral de Direito Civil**. Ano 4. Vol. 16, out-dez, 2003.

DOTTI, René Ariel. A liberdade e o direito à intimidade. In: **Revista de Informação Legislativa**: Brasília. Ano 17, n. 66, abr./jun. 1980.

_____. A tutela jurídica da privacidade. In: Estudos em homenagem ao professor Washington de Barros Monteiro. São Paulo: Saraiva, 1982

ETZIONE, Amitai. **Los limites de la privacidad**. Trad. Alexander López Lobo. Madrid, España: Edisofer S. L, 2012.

E.U.A. Freedom of Information Act. United States Department of Justice, 1967. Disponível em: http://www.justice.gov/oip/foi-act.htm. Acesso em 05/05/2014.

FACCHINI NETO, Eugênio. Reflexões histórico-evolutivas sobre a constitucionalização do direito privado. In: SARLET, Ingo Wolgang (org.). **Constituição, Direitos Fundamentais e Direito Privado**. Porto Alegre: Livraria do Advogado, 2003.

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

FERNANDES, Milton. Proteção civil da intimidade. In: **Revista do Instituto dos Advogados de Minas Gerais.** Minas Gerais: Inédita, 1996.

FERRAZ JUNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites a função fiscalizadora do Estado. In: **Cadernos de Direito Constitucional e Ciência Política**. São Paulo: Revista dos Tribunais, 1993.

FOROUZAN, Behrouz A. **Comunicação de dados e redes de computadores**. Porto Alegre: Bookman, 2006.

FOUCAULT, Michel. **Vigiar e punir**. Petrópolis: Vozes, 1988.

_____. **Microfísica do poder**. Trad. Roberto Machado. Rio de Janeiro: Edições Geral, 1979.

GERMAN, Cristiano. **O caminho do Brasil rumo à era da informação**. São Paulo: Fundação Konrad Adenauer, 2000.

GIORGIANNI, Michele. **O direito privado e suas atuais fronteiras**. São Paulo: Revista dos Tribunais, v. 747, ano 87, p. 35-55, jan. 1998.

GLANCY, Dorothy. **Privacy and the other Miss M. Summer, 1990**. Symposium on the right to privacy: after one hundred years, 10, n. Ill, U. L. Rev. 401. Disponível em: <http://migre.me/ciK8C>. Acesso em: 10 de dez/ 2014.

GODOY, Arnaldo Sampaio de Moraes. **Corte Constitucional alemã é formada pelo legislativo**. Disponível em: http://www.conjur.com.br. Acesso em 01 de jul. 2014.

GOMES, Orlando. **Introdução ao direito civil**. Rio de Janeiro: Forense, 2001.

GONÇALVES, Maria Eduarda. **Direito da informação** – Novos direitos e formas de regulação na sociedade da informação. Coimbra: Almedina, 2003

GROSS, Hyman. **The concept of privacy**. In: 43 New York University Law Review, 1967.

GUERRA, Sidney. **O direito à privacidade na internet**: uma discussão da esfera privada no mundo globalizado. Rio de Janeiro: América Jurídica, 2004.

HEGEL, George Wilhelm. **Grundlinien der Philosophie desRechts, Frankfurt am Main**: Suhrkamp, 1991.

HESSE, Konrad. **Derecho Constitucional y Derecho Privado**. Trad. Ignácio Gutierrez. Madrid: Civitas Ediciones, 1995.

ITÁLIA. **Codice in matéria di protezione dei dati personali**. Decreto legislativo 196, de 30 de agosto de 2003. Disponível em: http://www.parlamento.it/parlam/leggi/deleghe/03196dl.htm. Acesso em: 20/04/2014.

KANT, Immanuel. Fundamentação da Metafísica dos Costumes. In: KANT, Immanuel. **Os pensadores – Kant (II).** Trad. Paulo Quintela. São Paulo: Abril Cultural, 1980.

KONDER, Carlos Nelson. **Privacidade e corpo**: convergências possíveis. In: Revista Pensar, Fortaleza-Ce. V. 18, n. 02. p. 354, 2013.

LAZZARA, Paolo. **Autorità indipendenti e discrezionalità**. Padova: CEDAM, 2001.

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva 2012.

LOCKE, John. **Segundo tratado sobre o governo civil**: Ensaio sobre a origem, os limites e os fins verdadeiros do governo. Petrópolis: Vozes, 2005.

MARQUES, J. A. Garcia. **Informática e liberdade**. Lisboa, 1975.

MEDEIROS, Luciano Frontino de. **Banco de dados – princípios e prática**. Curitiba: IBPEX, 2007.

MEIRELLES, Jussara. O ser e o ter na codificação civil brasileira: do sujeito virtual à clausura patrimonial. In: FACHIN, Luiz Edson (coord.) **Repensando fundamentos do Direito Civil brasileiro contemporâneo**. Rio de Janeiro: Renovar, 1998.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. São Paulo: Saraiva, 2014.

MENEZES, Joyceane Bezerra de; GONÇALVES, Camila Figueiredo Oliveira. **Das fronteiras à interlocução entre os direitos da personalidade, os direitos fundamentais e os direitos humanos: elementos para construção da subjetividade.** In: Revista Jurídica Cesumar – Mestrado, v. 12, n.1, p. 175-203, jan/jun 2012.

MILLS, Jon L. **Privacy:** The lost right. New York: Oxford University Press. Kindle Editions. Ebook, 2008.

MILL, J. S.. **A Liberdade/Utilitarismo**. Martins Fontes, 2000, 278p.

MIRANDA, Pontes de. **Tratado de Direito Privado**. São Paulo: RT, 2000.

MIRANDOLA, Giovani Pico della. **Discurso sobre a Dignidade do Homem**. Lisboa: Edições 70, 1986.

MORAES, Maria Celina Bodin de. **A caminho de um Direito Civil-Constitucional**. Revista de Direito Civil. São Paulo, n. 65, jul-set 1993.

_____. **Na medida da pessoa humana**. Rio de Janeiro: Renovar, 2010.

NOJIRI, Sérgio. **O direito à privacidade na era da informática – algumas considerações**. Jur. UNIJUS, Uberaba: MG, V.8, nº 8, maio/2005, p. 99-106.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONUBR). **Direito à privacidade na era digital**. Disponível: http://www.onu.org.br/20013. Acesso em 01 de julho de 2014.

PEREIRA, Caio Mário da Silva. **Instituições de direito civil**. Rio de Janeiro: Forense, 2006.

PERLINGIERI, Pietro. **Perfis do Direito Civil**. Trad. Maria Cristina de Cico. Rio de Janeiro: Renovar, 2007.

PIANOVSKI, Carlos Eduardo. **Liberdade e função**: contribuição critica para uma nova fundamentação da dimensão funcional do Direito Civil brasileiro. Tese apresentada ao Programa de Pós-Graduação em Direito da Universidade Federal do Paraná. 2009. Disponível em: http://dominiopublico.mec.gov.br/download/teste/arqs/cp143683.pdf. Acesso em: 29/06/2014.

PINHEIRO, Patricia Peck. **Parecer- Contribuições para redação do Anteprojeto de Lei de Proteção de Dados Pessoais**. Disponível em: http://www.culturadigital/dadospessoais. Acesso em: 01 de jul. 2014.

PINTO, Paulo Mota. A limitação voluntária do direito à reserva sobre a intimidade da vida privada. **Revista Brasileira de Direito Comparado**. Publicação do Instituto de Direito Comparado Luso-Brasileiro: Rio de Janeiro, 2002.

_____. O direito à reserva sobre a intimidade da vida privada. In: **Boletim da Faculdade de Direito**: Coimbra, v. 69, 1993.

PONTES DE MIRANDA, Francisco Cavalcanti. **Tratado de Direito Privado**. Campinas: Bookseller, 2000.

PROSSER, William. "Privacy". In: **48 Califórnia Law Review 383 (1960).** Disponível em: http://www.californialawreview.org/.../prosser_privacy.pdf. Acesso em 15 de fev. 2014.

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

_____. **Tecnologie e diritti**. Bologna: Il Mulino, 1995.

_____. **Elaboratori elettronici e controllo sociale**. Bologna: Il Mulino, 1973.

RODRIGUES, Silvio. **Direito Civil**: Parte Geral. São Paulo: Saraiva, 2002.

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

SARLET, Ingo Wolfgang. **A dignidade da pessoa humana e os direitos fundamentais na Constituição Federal de 1988**. Porto Alegre: Livraria do Advogado, 2006.

SCHNEIER, Bruce. **Segurança.com – segredos e mentiras sobre a proteção digital**. Trad. Daniel Vieira. Rio de Janeiro: Campus, 2001.

_____. The future of privacy. In: **Scheneier on securiy**. 2006. Disponível em: <http://www.scheneier.com/blog/archives/2006/03/the_future_of_p.html>. Acesso em 09/03/2012.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. São Paulo: Malheiros, 2001.

SIVIERO, Fabiana Regina; CASTRO, André Zanatta de. Privacidade na era da revolução digital. IN: **Revista do Advogado**, ano. XXXII, n. 115, abril/2012

SOLOVE, Daniel J. **The digital person:** Thechnology and privacy in the information age. New York: New York University Press, 2004. Kindle Edition. Ebook.

_____. **A Taxonomy of Privacy**. University of Pennsylvania Law Review, Vol. 154, No. 3, p. 477, January 2006; GWU Law School Public Law Research Paper No. 129. Disponível em: <http://ssrn.com/abstract=667622>. Acesso em 16/03/2013.

SUNSTEIN, Cass. **The partial constitution**. Massachusetts: Havard Press, 1993.

SZANIAWSKI, Elimar. **Direitos da Personalidade e sua tutela**. 2. ed., rev., atual. e ampl.. São Paulo: Revista dos Tribunais, 2005.

TEPEDINO, Gustavo. A tutela da personalidade no ordenamento civil-constitucional Brasileiro. In: _____. **Temas de Direito Civil**. 3. ed., revista e atualizada. Rio de Janeiro: Renovar, 2004.

TOBEÑAS, José Castan. **Los Derechos de La Personalidad**. Madrid: Réus, 1952.

UNIÃO EUROPÉIA. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995. Jornal Oficial nº L281, de 23/11/1995. Disponível em: http:www.eurlex.europa.eu. Acesso em: 28/01/2014.

_____. **Convenção 108/1981 do Conselho da Europa**, de. Disponível em: http://www.cnpd.pt/bin/legis/internacional/Convencao108.htm. Acesso em: 23/03/2014.

_____. **Diretiva 97/66/CE do Parlamento Europeu e do Conselho de Europa**, de 15 de dezembro de 1997, relativa ao tratamento de dados pessoais e proteção à privacidade no setor das telecomunicações. Portugal: Jornal Oficial das Comunidades Europeias, 1998.

_____. **Diretiva 2002/58/CE do Parlamento Europeu e do Conselho da Europa**, de 12 de julho de 2002, relativa ao tratamento de dados pessoais no setor das comunicações eletrônicas. Portugal: Jornal Oficial das Comunidades Europeias, 2002

VASCONCELOS, Arnaldo. Todo direito natural é fundamental e humano. In: MENEZES, Joyceane Bezerra (Org.). **Dimensões jurídicas da personalidade na Ordem Constitucional Brasileira**. Florianópolis: Conceito, 2010.

VENEZUELA. **Constituição da República Bolivariana da Venezuela**.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade de informação**. Porto Alegre: Sergio Antonio Fabris, 2007.

WARREN, Samuel; BRANDEIS, **Louis. The right to privacy**. Harvard Law Review, vol. IV, n. 05, 1890. Disponível em: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html. Acesso em 10 de fevereiro de 2014.

WESTIN, Alan F. **Privacy and freedom**. New York: Atheneum Publishers, 1967. Ebook.