



UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS – CENTRO DE EDUCAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM GESTÃO NAS ORGANIZAÇÕES
APRENDENTES

TASSYARA ONOFRE DE OLIVEIRA

GESTÃO DE DADOS PESSOAIS: UMA ANÁLISE DE CASOS CONCRETOS A
PARTIR DO ORDENAMENTO JURÍDICO BRASILEIRO

JOÃO PESSOA
2017

TASSYARA ONOFRE DE OLIVEIRA

**GESTÃO DE DADOS PESSOAIS: UMA ANÁLISE DE CASOS CONCRETOS A
PARTIR DO ORDENAMENTO JURÍDICO BRASILEIRO**

Dissertação apresentada ao Programa de Pós-Graduação em Gestão Nas Organizações Aprendentes da Universidade Federal da Paraíba (UFPB), linha de pesquisa: *Gestão de Projetos Educativos e Tecnologias Emergentes*, como pré-requisito da obtenção do Título de **MESTRE**.

Orientador: Prof. Dr. Guilherme Ataíde Dias

JOÃO PESSOA
2017

Catálogo na publicação
Seção de Catalogação e Classificação

Oliveira, Tassyara Onofre de.
O48g Gestão de dados pessoais: uma análise de
casos concretos a partir do ordenamento jurídico
Brasileiro / Tassyara Onofre de Oliveira. - João
Pessoa, 2017.
108 f. : il.

Orientação: Guilherme Ataíde Dias.
Dissertação (Mestrado) - UFPB/CE.

1. Tecnologia da informação. 2. Dados pessoais -
Gestão. 3. Ordenamento jurídico - Brasil. I. Dias,
Guilherme Ataíde. II. Título.

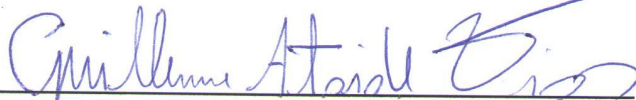
UFPB/BC

TASSYARA ONOFRE DE OLIVEIRA

**GESTÃO DE DADOS PESSOAIS: UMA ANÁLISE DE CASOS CONCRETOS A
PARTIR DO ORDENAMENTO JURÍDICO BRASILEIRO**

Aprovado em: 30 / 08 / 2017

BANCA EXAMINADORA

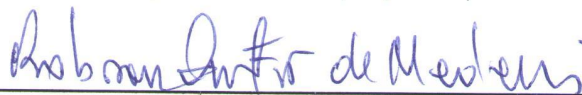


Prof. Dr. Guilherme Ataíde Dias
Orientador



Prof. Dr. Marckson Roberto Ferreira Dde Sousa
Examinador interno

Profa. Dra. Bernardina Maria Juvenal Freire de Oliveira
Examinadora interna (Suplente)



Prof. Dr. Robson Antônio de Medeiros
Examinador externo

“A percepção do desconhecido é a mais fascinante das experiências. O homem que não tem os olhos abertos para o misterioso passará pela vida sem ver nada.”

Albert Einstein

RESUMO

Investiga a proteção de dados pessoais no âmbito no ordenamento jurídico, com o intuito de desvendar qual o nível de tal tutela e como esta se efetiva. Para tanto, objetiva-se identificar a legislação brasileira que trata sobre a proteção de dados pessoais. Identificar quais os desafios para de gestão dados pessoais, apurar alguns casos práticos no âmbito nacional e internacional. Consequentemente, buscar soluções através da legislação e princípios já existentes no Brasil e no mundo para resoluções de casos. Por fim, mapear as legislações e práticas de outros países, comparando com as do Brasil, com o objetivo de apresentar novas soluções em que as leis brasileiras possuem uma lacuna. Quanto ao método, a pesquisa configura-se como qualitativa de cunho documental. Espera-se com essa pesquisa que ao fim, sejam identificadas as práticas de gestão de dados pessoais no Brasil.

Palavras chave: Dados pessoais. Tecnologia da Informação. Gestão. Ordenamento Jurídico Brasileiro.

ABSTRACT

This research investigates the protection of personal data within the Brazilian legal system, in order to unravel the level of protection and how this is effected. Therefore, the objective is to identify the Brazilian legislation that deals with the protection of personal data. Identifies the challenges for managing personal data in Brazil, establish some practical cases in the national and international levels. It aims, therefore, to seek solutions through legislation already regarded in Brazil for cases of resolutions. Finally, it maps the laws and practices of other countries, compared with those from Brazil, with the aim of presenting new solutions to the loopholes in Brazilian laws. As for the method, the research appears as qualitative primarily based on documentary evidence. It is hoped that this research, at its end, identifies personal data management practices in Brazil.

Keywords: Personal data, Information technology. Management. Brazilian legal system.

LISTA DE FIGURAS

Figura 1: Significação do dado.....	31
Figura 2: Comparação entre o Big Data e o Small Data.....	37
Figura 3: Teoria dos Círculos Concêntricos.....	65
Figura 4: Exemplo de um mosaico.....	67
Figura 5: Situação do Brasil no mapa de Proteção de Dados Pessoais no mundo.....	69
Figura 6: Print da tela inicial do site “Debate Sobre a Lei de Dados Pessoais no Brasil”.....	76

SUMÁRIO

1 CONSIDERAÇÕES INICIAIS.....	10
1.1 Objetivos	14
1.1.1 Objetivo geral	14
1.1.2 Objetivos específicos.....	14
1.2 Justificativa.....	14
2 CONSIDERAÇÕES METODOLÓGICAS.....	18
2.1 Delimitações do objeto	18
2.2 Caracterização da pesquisa	22
2.3 Fontes da investigação.....	24
3 DADOS PESSOAIS: CONCEITOS E DISTINÇÕES	25
3.1 Dado	25
3.1.1 Bancos de dados.....	27
3.1.2 Tratamento de dados	28
3.1.3 Violação de dados.....	29
3.2 Informação	29
3.2.1 Tecnologia da informação	31
3.2.2 Sociedade da informação.....	32
3.3 Dados pessoais	32
3.3.1 Dados anônimos	33
3.3.2 Dados sensíveis	33
3.3.3 Big data	34
3.3.4 Small data	36
4 PRINCÍPIOS PARA A PROTEÇÃO DE DADOS PESSOAIS.....	39
4.1 Os direitos subjetivos do titular dos dados pessoais	39
4.2 Princípios de proteção dos dados pessoais.....	41
4.2.1 Princípio da finalidade	42
4.2.2 Princípio da transparência.....	43
4.2.3 Princípio do consentimento	43
4.2.4 Princípio da lealdade ou boa-fé	45
4.2.5 Princípio da segurança física e lógica	46
4.2.6 Princípio da responsabilidade	47

4.2.7 Princípio da proibição de tratamento de dados sensíveis	48
4.3 O alcance dos princípios	50
4.4 Direitos de defesa do titular dos dados pessoais	51
4.4.1 Direito de acesso.....	52
4.4.2 Direito à retificação.....	52
4.4.3 Direito de vinculação a finalidade	53
4.4.4 O direito ao cancelamento.....	53
4.4.5 Direito ao esquecimento.....	54
4.4.6 Direito a não sujeição a decisões individuais automatizadas	56
5 A PRIVACIDADE: NOVOS CONTORNOS REFLETIDOS PELA SOCIEDADE DA INFORMAÇÃO	58
5.1 Tutela do direito a privacidade aos dados pessoais.....	62
5.1.1. Normas nacionais.....	62
5.1.2 Normas internacionais.....	64
5.2 Teorias da privacidade.....	64
5.2.1 Teoria dos círculos concêntricos (ou das esferas)	64
5.2.2 Teoria do mosaico	66
6.DADOS PESSOAIS SOB A ÓTICA DO ORDENAMENTO JURÍDICO BRASILEIRO	69
6.1 A proteção de dados pessoais no brasil.....	69
6.2 Projetos de leis para proteção dos dados pessoais no brasil	75
7. OS IMPACTOS NA GESTÃO DO DADOS PESSOAIS.....	79
7.1 Gestão de dados pessoais e direitos fundamentais: riscos e oportunidades	79
7.2 Âmbito de proteção.....	81
7.2.1 Dimensão subjetiva	82
7.2.2 Dimensão objetiva.....	84
8 ANÁLISES DOS CASOS CONCRETOS	86
8.1 Caso da smartv no Brasil	86
8.1.1 Análise do caso	87
8.2 O rastreamento de namorado	87
8.2.1 Análise do caso	88
8.3 O site tudo sobre todos	88
8.3.1 Análise do caso	89

8.4 Criptografia e legalidade.....	89
8.4.1 Analise do caso	89
8.5 Oi e vazamento de dados	90
8.5.1 Analise do caso	90
8.6 Falha no app do Banco do Brasil.....	91
8.6.1 Analise do caso	91
8.7 Colégio bandeirantes e vazamento de dados de alunos	92
8.7.1 Analise do caso	92
8.8 Acesso não autorizado de funcionários.....	93
8.8.1 Analise do caso	93
8.9 Privacidade do “Pokémon Go”	94
8.9.1 Analise do caso	95
8.10 Whatsapp integrado ao Facebook	95
8.10.1 Analise do caso	95
8.11 Aplicativos para controle do ciclo menstrual	96
8.11.1 Analise do caso	96
8.12 Vigilância estatal	97
8.12.1 Analise do caso	97
CONSIDERAÇÕES FINAIS	98
REFERÊNCIAS.....	101

1 CONSIDERAÇÕES INICIAIS

Os tradicionais locais públicos como praças, ruas, parques, aeroportos, centros comerciais assim como as próprias pessoas são submetidas cada vez mais a um controle efetivo de nossas ações. Passando por transformações onde não existe mais anonimato em meio à multidão. O momento atual caracteriza-se por inúmeras mudanças, influenciadas cada vez mais pelos avanços tecnológicos e consequentemente o surgimento de um novo modelo sociedade, marcada pela informação e o conhecimento. Atualmente é indiscutível a capacidade da Internet em dinamizar o contexto social, fazendo com que algumas questões sejam repensadas, frente aos novos desafios digitais. Dentre esses está o emergente anseio pela proteção de dados pessoais, em âmbito virtual, para além da autorregulação, até então recorrente no cenário brasileiro. Com o crescente acesso a web, uma efetiva proteção dos dados pessoais inseridos nesse novo meio demanda a regulação legal, de forma a tutelar direitos fundamentais da privacidade e intimidade. Tal pretensão deve ser vista como uma alternativa de maximizar a proteção aos referidos direitos e não como uma tentativa de restrição a liberdade informática. Essa nova era é chamada de Sociedade da Informação, termo difundido e conceituado por Machlup (1962)¹, tem como marco a década de 80 (CASTELLS, 1999)² e está ligada a expansão, reestruturação do capitalismo e dedicado aos estudos da ação social nesse ambiente tecnológico, em que se destaca a Internet apresentando as redes digitais seu símbolo maior.

No ciberespaço, podemos perceber que privacidade e o controle na Internet estão diariamente se confrontando, nesse universo são figuras antagônicas. Nesse ambiente não existem dados pessoais privados ou públicos, bons ou ruins, úteis ou inúteis. Todos são capturados e armazenados, pois nada se perde. Quando são agrupados, somados e devidamente tratados esses dados permitem que sejam traçados perfis precisos dos indivíduos. Nossos dados se tornaram as novas *commodities*. A proteção de dados pessoais surge para a prevenção e as demandas

¹ No artigo *The Production and Distribution of Knowledge in the United States* (A produção e distribuição do conhecimento nos Estados Unidos), de 1962, no qual é creditado com popularização o conceito de sociedade da informação.

² As novas tecnologias difundiram-se pelo globo com a velocidade da luz em menos de duas décadas, entre meados dos anos 70 e 90, por meio de uma lógica que (...) é a característica dessa revolução tecnológica: a aplicação imediata no próprio desenvolvimento da tecnologia gerada, conectando o mundo através da tecnologia da informação. (CASTELLS, 1999, p. 52).

que necessitam deliberações no âmbito da sociedade da informação, por exemplo, como contra os potenciais riscos de serem causados pelo tratamento de dados ou como o uso indevido dos dados coletados. Originando a possibilidade de tutelar a personalidade do indivíduo nesse universo. Partindo dessa apreensão, que se passa a desenvolver o presente trabalho, sendo o primeiro momento destinado à explanação do direito fundamental a privacidade, que após o advento da Internet e a inserção de dados pessoais nesse âmbito virtual, deparou-se com um novo contexto desafiador, de onde decorrem conflitos a serem observados e abarcados pelo âmbito jurídico para garantir o referido direito.

Diferente da perspectiva preponderantemente econômica, o presente trabalho descreve-se o anteprojeto de lei brasileira de proteção dos dados pessoais, que pretende proteger o internauta da possível vulnerabilidade conferida aos seus dados. O objetivo não é de proteger os dados apenas, mas sim, o titular desses dados de organizações, sejam elas públicas ou privadas. Tendo em vista que os dados pessoais constituem-se intermediários entre a pessoa e a sociedade, a personalidade de um indivíduo pode ser gravemente violada com a divulgação imprópria e a utilização de dados armazenados a seu respeito. Por se constituírem em uma parcela da personalidade da pessoa, os dados pessoais merecem tutela jurídica, de modo a assegurar sua liberdade e igualdade. Ao se analisar o tema da proteção de dados pessoais na sociedade da informação, é essencial compreender que o cerne do problema não se encontra na tecnologia. Afinal, no debate sobre proteção de dados pessoais, é de entendimento que a própria tecnologia é criada pela sociedade para atingir determinados fins e o grau de sua regulação é estabelecido pela sociedade que a criou. Neste momento, vêm-nos à mente a primeira Lei de Kranzberg, pinçada do primeiro capítulo da obra de Manuel Castells (p. 59, 2001), “a tecnologia não é boa nem ruim e também não é neutra. É uma força que provavelmente está, mais do que nunca, sob o atual paradigma tecnológico que penetra no âmago da vida e da mente”. Quem faz o uso dela determina sua finalidade.

A tecnologia interage, necessariamente, com toda a sociedade. Contudo, os resultados desta interação diferem em função dos contextos econômicos, sociais, políticos, culturais, demográficos e temporais específicos. Ou seja, não é a tecnologia em si que causa problema da privacidade, mas sim as decisões que

tomamos em relação ao uso dos meios tecnológicos. Com isso, fica claro que a sociedade da informação somente poderá obter vantagens do desenvolvimento tecnológico se este for acompanhando da gestão jurídica de privacidade. Garantindo ao titular dos dados pessoais a autonomia das suas escolhas, como também, a sua dignidade e a tutela de personalidade.

A proteção de dados é uma disciplina que está ligada a privacidade. Mas, de antemão não se pode confundir com o Direito a Privacidade, que está ligado a personalidade e de natureza claramente subjetivo. O qual depende muito de condições particulares como o tempo, classe, condição social, econômica e outros fatores subjetivos. Portanto, o direito a privacidade não tem como garantir a regulação de proteção de dados pessoais. Por isso existe a necessidade de regras claras, inseridas não só para os aplicadores do direito, mas que também possam ser executadas por sistemas informatizados que tratam os dados e que tenha em sua concepção a noção do que pode ser feito ou não feito com as informações pessoais. O direito a privacidade pode sim servir de base normativa, mas não tem a dinâmica necessária, dado a velocidade e quantidade de vezes que essas informações podem ser tratadas em um curto espaço de tempo.

A modernidade permite que a pessoa seja identificada por reconhecimento facial, tenha seu nome vasculhado na Internet, em tempo real, e sua vida revirada nos sites de relacionamento, nas opiniões e comentários que postou e nos demais dados espalhados em redes e banco de dados. Esses dados são reunidos e minerados por sofisticados programas. Apresentando aspectos de sua personalidade e seu comportamento, e até tração possibilidades de suas futuras atitudes. A segurança da informação tornou-se agora é importante para todos. Também se tornou universal a intrusão ofensiva por meio eletrônico, não apenas mais democrática. Qualquer um pode praticar ofensa no mundo virtual, não importa onde esteja. Esse fenômeno, aliás, tornar em pouco tempo uma pessoa mundialmente conhecida.

Direito de defesa e proibições de condutas específicas podem e devem ser utilizados pelos operadores do direito. As medidas preventivas tem lugar nessa seara. A reparação pecuniária, não apenas de danos materiais e morais, mas também daquele existencial que afeta de maneira substancial a vida da pessoa, tem

um lugar especial na tutela dos direitos da personalidade. Os danos podem ser transnacionais, mas, em regra, o direito aplicado é nacional quando decorrente de prestação de serviços realizados no Brasil. Desafios próprios aparecem no percurso. A lesão ocorrida na Internet ainda carece de uma solução técnica perfeita, não apenas restrição de informação ilícita com a retirada do conteúdo. Existem desafios processuais que essa tutela específica traz em seu bojo, como a questão da competência, inclusive internacional, em que se deve interpretar a mais afeta ao acesso à Justiça e a defesa dos direitos fundamentais.

A privacidade dos dados pessoais é a última fronteira entre o público e o privado. É nela que o cidadão é formado, com suas crenças, subjetividades, opiniões, frustrações, esperanças e pensamentos. É a partir dela que surge a diversidade cultural, étnica, religiosa, sexual, artística, filosófica e científica, que nos faz diferente de qualquer outra espécie. Preservar a privacidade dos dados pessoais na sociedade da informação não é um luxo, mas uma necessidade.

Parte da doutrina e da jurisprudência nacional ainda não compreendeu a dimensão do problema. Análise de questões como dados financeiros, uso de rastreadores, de localização geográfica, captação de áudio visual e em geral. Procura-se normalmente julgar o caso concreto, mas não a reflexão sistêmica dos riscos e princípios que estão intimamente ligados a exposição dos dados pessoais. Parte da doutrina jurídica nacional desconhece o potencial lesivo da mineração de dados. Também o legislativo ainda está inerte indisciplinar razoavelmente a matéria. Imprescindível reconhecer os princípios afetos os dados pessoais, consolidar o entendimento de que há um direito fundamental à proteção de seus dados. Para elaborar este trabalho, observou-se o contexto acima exposto, referentes ao momento brasileiro relacionado à proteção de dados pessoais inseridos na Internet, que não se encontra definido, pois na inexistência de Lei protetiva, o momento apresenta-se auto regulatório, mas na perspectiva de regulação, em decorrência do Anteprojeto de Lei de Proteção de Dados Pessoais. Diante dessa situação, a sociedade informacional brasileira, oscila em auferir efetiva proteção ou deixar “nas mãos do mercado” a elaboração de normas para tanto, oscilando entre regulação e autor regulação, ambos os contextos evidenciados através do procedimento comparativo.

Diante do que foi exposto, surge uma inquietação que poderia se exprimir na seguinte questão: De que forma se configuram as formas de Gestão dos dados pessoais no contexto brasileiro?

1.1 Objetivos

Assim, esse estudo tem como objetivos:

1.1.1 Objetivo Geral

Analisar o contexto da Gestão de dados pessoais no Brasil.

1.1.2 Objetivos Específicos

Para alcançar o objetivo geral, são considerados os seguintes objetivos específicos:

- Identificar os principais conceitos e peculiaridades sobre os Dados Pessoais;
- Mapear a legislação sobre o tema;
- Discutir casos concretos sobre Gestão dos Dados Pessoais.

1.2 Justificativa

Ao longo do processo de minha formação acadêmica e profissional enquanto jurista, sempre me interessou os debates em torno dos problemas que dizem respeito à Propriedade Intelectual (PI) onde se inserem os direitos do autor, direitos relativos à propriedade industrial e a proteção dos Sui Generis. Embora não seja um tema explorado com a profundidade no Curso de Direito, muitas vezes, nenhuma matéria específica é oferecida na matriz curricular da graduação relativa ao tema, tive a oportunidade de ser apresentada ao conteúdo apenas pela reflexão associada aos estudos de outras disciplinas. Sempre me chamando atenção, as leituras que envolviam o Direito Civil, Direito Comercial e o Direito Internacional, mas não os bens propriamente tangíveis, mas sim os bens intangíveis, associados aos produtos de informação. Consecutivamente me relevavam como são importantes as leis, questões éticas e jurídicas sobre o tema, e também na esfera internacional nunca

deixando de dar atenção aos tratados que remetem ao problema, que são de extrema importância nas relações internacionais e nas resoluções de conflitos.

Estudos mais aprofundados já no mestrado principalmente nas disciplinas de linha de pesquisa tive a oportunidade de ter maior contato com novos objetos de estudo, me abrindo a oportunidade de poder aprofundar minha compreensão sobre aspectos jurídicos relevantes, me motivando a desenvolver a proposta deste trabalho. Principalmente sobre o papel fundamental da informação na sociedade contemporânea, no âmbito social e econômico. Pois, as mudanças tecnológicas ocorrem em tal progressão geométrica, repentinamente, o que era inovador, logo se torna obsoleto.

Com a velocidade da transmissão da informação não é diferente. No cenário atual, caracterizado por um mundo globalizado e altamente tecnológico, surgem novas trajetórias, modos e distintas formas de aprendizagem em função das inovações ocorridas na construção, compartilhamento e difusão do conhecimento. Tais transformações possibilitaram não somente uma nova maneira de acesso à informação, mas, também, modificações profundas nos costumes, hábitos e nas culturas de vários povos, que ultrapassaram os limites locais e romperam as barreiras transnacionais.

Se de fato existe uma estrutura que permite esse avanço aos limites da privacidade, estes são os denominados bancos de dados, através de Sistema de Gerenciamento de Banco de Dados – SGBD (*Data Base Management System - DBMS*):

Sistema de Gerenciamento de Banco de Dados capaz de utilizar recursos computacionais fortemente acoplados (processadores, discos e memória). [...] a tecnologia de banco de dados paralelo promete melhoria de desempenho e alta disponibilidade, mas problemas de interoperabilidade se não gerenciada adequadamente. (MANNINO, 2008, p. 693)

O processamento é feito por grandes organizações privadas e públicas, com o objetivo de ordenar, tratar e classificar os dados. Diante de capacidade das organizações de armazenamento de dados, o valor e o papel da informação perante a sociedade é crescente.

Consequentemente, ganha àquele que dominar o conhecimento das tecnologias da informação. Não somente em quantidade de dados tratados, mas pela qualidade processamento. Os bancos de dados se tornam um instrumento perfeito para ultrapassar os limites da privacidade. Pois na sociedade da informação, a proteção de dados pessoais diverge em vários aspectos do tradicional direito à privacidade. Não existem mais territórios, somos dependentes dos dispositivos pós-PC, ou como normalmente chamamos, os dispositivos móveis, pela conveniência e a praticidade, por nos acompanharem todo tempo, e auxiliarem nossas vidas com suas funções e aplicativos. Estamos todo tempo conectados a rede, seja para trabalho, estudo ou simplesmente diversão. Somos os nossos dados, eles nos determinam, nos rotulam por meio de nossos acessos e escolhas. Uma rede que não é apenas só virtual, pois, se confunde com o real e o ambiente se funde em uma só esfera.

Controlar a circulação dos nossos dados, saber quem os usam e com qual finalidade, poder acessá-los a qualquer tempo, editá-los e removê-los. Esses atos significam ter poder sobre si na sociedade da informação, o acesso a dados pessoais ultrapassa o poder de escolha que delimita e define a esfera pessoal de cada ser humano, desnudando o mais íntimo de forma avassaladora. Vivemos em uma realidade onde tudo o que necessitamos é arquitetado, inventado, desenvolvido, produzido e vendido por as empresas. As inovações tecnológicas, principalmente nas telecomunicações e na informática, promoveram o processo de globalização. A partir da rede de telecomunicação foi possível a difusão de informações entre as empresas e instituições financeiras, ligando os mercados do mundo.

Ao preencher um cadastro em algum site, diariamente os consumidores fornecem as empresas dados como estado civil, nome dos pais, telefone, local de trabalho, e-mail e algumas vezes até a sua renda mensal, não apenas isso, o simples uso do celular geram dados pessoais que são capturados pelas empresas/governos. Assim como exemplificam Dias e Vieira:

Um indivíduo que utilize um smartphone deixa uma trilha de dados por onde quer que passe. Um smartphone gera informações de localização que podem ser captadas pela operadora de celular e eventualmente pelas aplicações instaladas no dispositivo, sendo possível assim traçar um mapa de deslocamento do usuário. (DIAS e VIEIRA, 2013, p.176)

O que muita gente não sabe é que esses dados podem estar sendo comercializados sem o seu consentimento. O valor de nossos dados pessoais nunca foi tão subestimado por nós. Beal (2009) alertou sobre a importância, que não se trata apenas de um amontoado de bytes, mas sim de um conjunto de dados organizados e classificados corretamente para que pessoa ou uma empresa possa utilizar conforme for necessário. Que quando são ordenados de maneira lógica e racional, se tornam informação, logo mais será aprofundado o conceito.

A informação pode determinar a continuidade ou a descontinuidade das atividades de uma organização, reiterando a importância dos dados pessoais. A informação é um patrimônio, ela agrega valor a qualquer organização. Por todos estes fatores, é fundamental a tutela jurídica para aqueles que confiam seus dados pessoais a entidades públicas ou privadas se torna evidente na medida em que esses dados possuem um valor econômico. O direito a proteção dos dados pessoais se apresenta claramente como um artifício fundamental para assegurar a liberdade, cidadania e igualdade.

2 CONSIDERAÇÕES METODOLÓGICAS

Habitualmente o conhecimento científico emerge a partir de inquietações e questionamentos.

No processo de construção do problema e do próprio conhecimento científico, esta inquietação será o “motor” que conduzirá o pesquisador no seu levantamento de dados, na busca por uma “resposta” - a hipótese - que deverá estar embasada em um marco teórico, em um quadro de leitura que permita ao leitor relacionar este tripé – problema/hipótese/marco teórico - de forma coerente e sistematizada (XIMENES, p.3, 2015)

Sendo assim, os procedimentos metodológicos são uma ferramenta indispensável para oferecer um norte à pesquisa científica. Pois, tem a função de como percorrer “o caminho das pedras”. O êxito de uma pesquisa depende necessariamente das abordagens, técnicas e processos e o cumprimento das etapas demandadas no processo, de uma maneira sistemática.

De acordo com Richardson:

não existe uma fórmula mágica e única para a realização de uma pesquisa ideal, uma vez que a investigação é um produto humano, e seus produtores são falíveis, exigindo-se, assim, necessário conhecimento da realidade, noções de metodologia, técnicas de pesquisa e um sério trabalho.(p.25, 1999)

Diante exposto, será apresentado no capítulo os motivos que deram origem ao problema.

2.1 Delimitações do objeto

Para Pierre Lévy (2011), é evidente a grande influência do ambiente virtual em todas as esferas da sociedade, categorizando transformações nunca dantes vistas no curso histórico da humanidade. Neste sentido de virtualização da vida humana é algo que envolve toda a sociedade global:

Um movimento geral de virtualização afeta hoje não apenas a informação e a comunicação, mas também os corpos, o funcionamento econômico, os quadros coletivos da sensibilidade ou o exercício da inteligência. A virtualização atinge mesmo as modalidades do estar junto, a constituição do “nós”: comunidades virtuais, empresas virtuais, democracia virtual. Embora a digitalização das mensagens e a extensão do ciberespaço desempenhem um papel capital na mutação em curso, trata-se de uma onda de fundo que ultrapassa amplamente a informatização. (LÉVY, 2011, p. 11)

A sociedade atual é globalizada e tecnológica, novos caminhos e desafios são colocados à vida em sociedade. Estamos vivendo atualmente a chamada sociedade em rede, onde não há limites para que a informação possa alcançar seus objetivos (CASTELLS, 1999). Hoje em dia o mundo cada vez mais se digitaliza, o tempo inteiro é gerado conteúdo digital, a geração de dados é cada vez maior e mais acelerada. A sociedade da informação ou sociedade do conhecimento, entre outras expressões apareceram para denominar essa nova fase que nossa sociedade vem evoluindo, são o suficiente para constatar o papel fundamental que a informação já exerce na sociedade em rede. Fundamental também é reconhecer o papel que desempenha na sociedade e a importância de buscar maneiras de lidar com esse fato e suas implicações no mundo atual. Diversas são as possibilidades de comunicação e acesso ao conhecimento, através de conexões e saberes compartilhados, possibilitam inúmeras direções, difundindo o conhecimento e informação.

A informação sempre foi valorizada na história humanidade. Guerras foram vencidas por exércitos que a tinham sob seu domínio. Reinos foram evitados de cair devido à mesma ser utilizada em momentos adequados. Milhões de mortes podem ser evitadas quando no tempo certo populações são informadas de algum fenômeno natural ou uma doença se aproxima, um exemplo é o Google Flu Trends³ que pode detectar e prevenir contra surtos de gripe. Já existe também o Google Dengue Trends⁴, que tem a função de alertar sobre os principais surtos de dengue no mundo, um problema presente em nosso país. Com a evolução tecnológica dos meios de comunicação, além da concorrência entre estes, o que predomina e move a comunicação informativa contemporânea é totalmente contraposto ao que em outros tempos valorizou a informação e a fez um objeto, e, muito valioso.

³ “O Google Flu Trends (*Google Tendências de Gripe*) disponibiliza, através de dados agregados de pesquisa online, uma estimativa da atividade de gripe em determinada região. Com essa ferramenta é possível detectar onde estão os pontos mais críticos ou que podem ser caracterizados como um tipo de epidemia.”

Revista Galileu. Google pode ajudar no controle da gripe. Disponível:

<<http://revistagalileu.globo.com/Revista/Common/0,,EMI288897-17770,00->

GOOGLE+PODE+AJUDAR+NO+CONTROLE+DA+GRIPE.html> Acesso em: 03 de outubro 2017.

⁴ “Google Dengue Trends are no longer publishing current estimates of Flu and Dengue fever based on search patterns”

Google Dengue Trends - <Disponível em: <https://www.google.org/flutrends/about/>> Acesso em: 03 de outubro 2017.

Presente em diversas áreas jurídicas: seja o direito penal, com a proteção contra informações como injúria ou difamação; o direito comercial com a garantia do sigilo empresarial e propriedade industrial e o tão fundamental para qualquer Estado, o direito constitucional, garantindo os direitos fundamentais como a liberdade de expressão, de imprensa e entre outros direitos, que serão tratadas ao longo do texto. Normas de direito tão antigas, mas que já reconheciam a importância de proteger a informação, na vida da sociedade e dos indivíduos.

O século XX, com a revolução digital, das formas de comunicação e da informação, gerou um desafio único para sistema legal. A regulação jurídica dessas entidades tão recentes e ainda pouco compreendidas. Mesmo assim, essa nova forma de informação e a comunicação transcorrem por todos os aspectos de nosso cotidiano, dos indivíduos e da sociedade. Algo tão presente no cotidiano que resultou no conceito de ubiquidade dos meios informáticos ou computação pervasiva (*Ubiquitous Computing ou ubicomp*), citado pela primeira vez por Mark Weiser (p. 94, 1991)⁵, descrevendo a onipresença da informática no cotidiano das pessoas. São diversos os elementos que representam essa ubiquidade como os smartphones, a Internet em nuvem, a Internet das coisas (IOT) e etc. Com todos esses novos recursos de comunicação, facilitação da vida com a tecnologia e da circulação de conhecimento, surgiu conjuntamente um maior controle social, a exposição indesejada e a restrição espontaneidade individual (intimidade, imagem, dados pessoais).

Um dos mais recentes e com maior repercussão casos de invasão de privacidade por parte do Estado foi o caso Snowden⁶, que revelou casos de espionagem nos EUA e gerou crise para o governo Obama, perante todo o mundo. Abalando a confiança de todos os cidadãos que se viram expostos, expondo um Estado que ao invés de proteger a integridade e o sigilo das informações que circulam pelos meios tecnológicos, as viola. Essa sociedade em rede exhibe uma nova visão de Estado, que vigia seus cidadãos cada vez mais, e com mais facilidade com o amparo da ubiquidade e a utilização dos cidadãos das mais diversas tecnologias, com um enfoque nos smartphones. Provocando um debate sobre privacidade na rede por todo o mundo, e revivendo um receio de um Estado como

⁵ WEISER, Mark. The Computer for the 21st Century.

⁶ GREENWALD, 2014.

um Big Brother⁷, que tudo quer saber, controlar e ver. Analisaremos diversos casos no Brasil e no mundo.

O desafio do Direito não pode ser maior, esse complexo cenário nos faz refletir a respeito da garantia da privacidade e da intimidade do indivíduo, que agora está fortemente vinculado às modificações tecnológicas e sociais. Motivando novos conceitos, transformações e discursões sobre. Na sociedade da informação, o direito à privacidade voltou-se para o risco a milhares de cidadãos cujos dados pessoais são diariamente coletados, processados por órgãos estatais e privados, com o auxílio de modernas tecnologias. Consequentemente, proteção de dados pessoais é qualitativamente diferente do tradicional direito à privacidade e o alavanca dessas mudanças é exatamente o uso intenso e inovador das tecnologias.

Nós somos os nossos dados, através deles podem nos definir e nos classificar, além de nos proporcionar também acessos de produtos e serviços, privados e públicos. Inúmeros são os dados que podem ser armazenados sem nosso conhecimento e sem nenhuma garantia de que serão utilizadas de maneira ética, e ainda compartilhadas sem que concordemos. O conhecimento que é gerado da informação de nossos dados pessoais são ativos intangíveis e abundantes, sendo assim, o conhecimento gerando pela coleta de informações pode ser usado por mais pessoas sem que se reduza o estoque. Com isso, abre-se um gigantesco potencial de enriquecimento com o processamento de dados. O armazenamento e análise de todo e qualquer dado na Internet pode ajudar a traçar comportamentos e tendências.

A revolução digital e suas novas tecnologias estabeleceu um contexto em que as questões sobre a privacidade precisam ser repensadas. Se por um lado acessar informações de órgãos públicos ficou mais fácil, à coleta de informações através os dados pessoais que anteriormente eram particulares, agora estão soltos na rede. Isso sem nenhuma autorização dos seus reais titulares. O avanço sobre o tema é extremamente importante, não podemos tentar interferir. Porém, gestão jurídica e controle de processos são indispensáveis para um equilíbrio entre todos os sujeitos nessa sociedade tão atual e inovadora. Pois os dados circulando na rede

⁷ Expressão citada por George Orwell em sua obra 1984.

são universais e os impactos também. Precisamos ponderar sobre isso. Analisar sobre o que já está em vigência na nossa legislação e o prevista para regular os Dados Pessoais no Brasil.

A importância do tema em questão – o estudo do uso de que se trata de um fenômeno que permeia o mundo moderno e está presente, mais que nunca, nas relações humanas e comerciais, que veio transformar e incrementar o universo tecnológico do século XX. A presente dissertação trata da evolução cibernética e de seus nichos e desdobramentos exploratórios, advindos do uso dos dados pessoais e as suas consequências no campo social e jurídico.

2.2 Caracterização da pesquisa

Considerando os objetivos propostos, será desenvolvida uma pesquisa com abordagem qualitativa. Pretende-se abordar o mundo, entender, descrever e às vezes explicar os fenômenos sociais de dentro, analisando experiências de indivíduos ou grupos, examinando as interações e comunicações em desenvolvimento ou analisando documentos. Minayo & Minayo-Gómez (2003, p.118), explicam que:

- 1) Não há nenhum método melhor do que o outro, o método, “caminho do pensamento”, ou seja, o bom método será sempre aquele capaz de conduzir o investigador a alcançar as respostas para suas perguntas, ou dizendo de outra forma, a desenvolver seu objeto, explicá-lo ou compreendê-lo, dependendo de sua proposta (adequação do método ao problema de pesquisa); 2) Os números (uma das formas explicativas da realidade) são uma linguagem, assim como as categorias empíricas na abordagem qualitativa o são e cada abordagem pode ter seu espaço específico e adequado; 3) Entendendo que a questão central da cientificidade de cada uma delas é de outra ordem [...] a qualidade, tanto quantitativa quanto qualitativa depende da pertinência, relevância e uso adequado de todos os instrumentos

Segundo Chizzotti (1995, p.11), “a pesquisa investiga o mundo em que o homem vive e o próprio homem”. Contudo, a pesquisa só existe com o apoio de procedimentos metodológicos adequados, que permitam a aproximação ao objeto de estudo. Na pesquisa qualitativa, o cientista é ao mesmo tempo o sujeito e o elemento de suas pesquisas.

Para Oliveira, “a pesquisa tem por objetivo estabelecer uma série de compreensões a fim de construir respostas para as indagações e questões levantadas nos diversos ramos do conhecimento humano” (2002, p. 62). Na presente dissertação, a metodologia utilizada ao longo da construção da pesquisa foi exploratória, aliada a uma reflexão crítica, permitirá um melhor entendimento e uma abordagem inovadora sobre o tema. Uma pesquisa exploratória, pois, existe a busca de se familiarizar com um assunto ainda pouco conhecido e explorado em nosso país. Com o objetivo de conhecer melhor sobre o assunto de proteção à privacidade e aos dados pessoais no Brasil, procurando construir hipóteses e soluções.

Por fim, no que tange os procedimentos empregados, essa pesquisa também será de cunho documental. Segundo Pádua (1997, p.62):

Pesquisa documental é aquela realizada a partir de documentos, contemporâneos ou retrospectivos, considerados cientificamente autênticos (não fraudados); tem sido largamente utilizada nas ciências sociais, na investigação histórica, a fim de descrever/comparar fatos sociais, estabelecendo suas características ou tendências

Mas o que significa a palavra “documento”? Uma forma de analisar o conceito é buscarmos por uma definição:

Documento: 1. declaração escrita, oficialmente reconhecida, que serve de prova de um acontecimento, fato ou estado; 2. qualquer objeto que comprove, elucide, prove ou registre um fato, acontecimento; 3. arquivo de dados gerado por processadores de texto” (HOUAISS, p.260, 2008).

O uso da pesquisa documental é justificada pelo uso de diversos documentos para elaboração da pesquisa. O documento como fonte de pesquisa pode ser escrito e não escrito, tais como filmes, vídeos, slides, fotografias ou pôsteres. Esses documentos são utilizados como fontes de informações, indicações e esclarecimentos que trazem seu conteúdo para elucidar determinadas questões e servir de prova para outras, de acordo com o interesse do pesquisador (FIGUEIREDO, 2007). Ainda, foram utilizadas na pesquisa diversas leis internacionais que em nosso país são pouco conhecidas, por ainda se tratarem de projetos de lei. Logo, material analisado não recebeu tratamento analítico.

De acordo com Gil (2002, p.62-3), a pesquisa documental apresenta algumas vantagens por ser “fonte rica e estável de dados”: não implica altos custos, não exige contato com os sujeitos da pesquisa e possibilita uma leitura aprofundada das

fontes. Ela é semelhante à pesquisa bibliográfica, mas se diferencia pela a natureza das fontes, sendo material que ainda não recebeu tratamento analítico, ou que ainda pode ser reelaborado de acordo com os objetivos da pesquisa.

2.3 Fontes da investigação

Serão utilizadas fontes de informações impressas secundárias, como livros, artigos, dissertações e teses sobre os temas, publicados em bancos de dados nacionais e internacionais sobre Dados Pessoais no Brasil, em língua portuguesa e inglesa. A fonte utilizada é, em grande parte, bibliográfica e documental. Foram incluídas, nesse primeiro momento, referências no âmbito da Sociedade da Informação; Privacidade e Cibercultura, para contribuir com os conceitos.

Foram utilizadas também as legislações e jurisprudências nacionais e de outros países sobre o assunto, a exemplo dos Estados Unidos, Portugal e Alemanha.

3 DADOS PESSOAIS: CONCEITOS E DISTINÇÕES

Nesse capítulo serão apresentados alguns conceitos e distinções sobre a Gestão Jurídica dos Dados Pessoais.

3.1 Dado

Os modernos aparelhos eletrônicos utilizados por bilhões de pessoas em todo o mundo trabalha a partir um elemento fundamental: o dado. Etimologicamente, dado vem da expressão latina datum utilizada para referir-se a qualquer coisa dada para alguém. Dentre as várias concepções existentes, define-se dado como sendo o registro que representa um fato, um conceito, uma instrução, um elemento ou um atributo de uma pessoa, entidade ou coisa. E se o dado não tem relevância ou propósito. O dado pode ser formado por um ou mais caracteres letras números palavras textos imagens vídeos Sons ou áudios. Valdemar Setzer, no artigo intitulado Dado, informação, conhecimento e competência, define dado como uma entidade puramente matemática, algo sintático:

Definimos *dado* como uma sequência de símbolos quantificados ou quantificáveis. Portanto, um texto é um dado. De fato, as letras são símbolos quantificados, já que o alfabeto por si só constitui uma base numérica. Também são dados imagens, sons e animação, pois todos podem ser quantificados a ponto de alguém que entra em contato com eles ter eventualmente dificuldade de distinguir a sua reprodução, a partir da representação quantificada, com o original. É muito importante notar-se que qualquer texto constitui um dado ou uma sequência de dados, mesmo que ele seja ininteligível para o leitor. (SETZER,1999,p.2)

Dados isolados como definido por Setzer(1999, p.2) não são prescindíveis de proteção, por serem apenas dados soltos, sem nenhum significado específico. Mas quando esses dados são agrupados, tratados e armazenados, se gera uma informação, reportando algum valor a “agrupado de dados”. Trataremos aqui sobre os Dados Pessoais, que basicamente é todo e qualquer dado que possa ligar a uma pessoa, dados esses que atualmente valem muito, por isso toda essa discursão para a proteção e garantia para que cada cidadão possa determinar de maneira autônoma a utilização que é feita de seus próprios dados.

Stair e Reynolds (2002, p. 4), reforçam o conceito, descrevendo que dados constitui apenas em fatos não trabalhados, desta forma, logo, quando esses fatos

são organizados ou ordenados, deforma a criar significado, tornam-se informação. Warcks (1989, p.25) esclarece:

Se o dado assume a forma de uma palavra impressa ele é imediatamente compreendido como informação para o leitor. Se, no entanto, o dado consiste em atos ou sinais que requeiram a interpretação antes de adquirirem qualquer sentido, ele permanece no estado de pré-informação até poder ser efetivamente compreendida por alguém.⁸ **(Tradução nossa)**

O fenômeno da informatização vem ganhando cada vez mais espaço na sociedade atual, ao passo de ser inconcebível, hoje, uma empresa, um governo, uma escola, que não esteja informatizada, para citar apenas alguns exemplos. Informatizar virou sinônimo de eficiência gerencial, redução de custos, maior produtividade, maior e melhor controle sobre as operações desenvolvidas e maior precisão.

Alimentar, com dados, os milhares de computadores distribuídos pelo mundo é a grande prioridade do homem no momento, bem como transformar esses dados em informação diferenciada e conseqüentemente valiosa. Stair constata tal fenômeno assim consignando:

Todos os dias somos solicitados a divulgar dados sobre nós mesmos. Na maioria das vezes, o fazemos sem pensar duas vezes. Aceitamos a solicitação como necessária, e, mais importante, os dados serão usados apenas para a finalidade para a qual foram fornecidos. O que não conseguimos perceber é que, atualmente, mais do que nunca, nossos dados estão sendo processados e compartilhados, muitos deles sem a nossa permissão ou conhecimento. As empresas descobriram que a venda de dados é um negócio lucrativo. Infelizmente, os dados que elas vendem são nossos. Dados demográficos, sobre tendências de compras e preferências pessoais tornaram-se valiosos para as organizações que tentam vender seus produtos em um mercado altamente competitivo. Por esta razão, a indústria de dados é muito lucrativa (1998, p. 122)

Mesmo em ampla quantidade, os dados são facilmente coletados e armazenados, pois a cada dia novas tecnologias e métodos são desenvolvidos para o tratamento de dados. Porém, o dado precisa de valor por ser um evento fora do contexto e sem significação para o sistema. Para que os dados se tornem úteis como à informação é necessário que a pessoa possa correlacioná-los e atuar sobre eles. Para tanto, a utilidade dos bancos de dados informatizados é notória. Através

⁸ *If the data is in the form of a printed word it is immediately understood as information for the reader. If, however, the data consists of acts or signals that require interpretation prior to purchase either direction, it remains in the pre-information can even be effectively understood by someone.*

destes é possível recolher um grande número dados, processá-las, agrupá-las e relacioná-las das mais diferentes formas e em tempo insuficiente. Todas essas possibilidades traduzem-se na palavra tratamento.

3.1.1 Bancos de dados

Os dados podem ser organizados, agrupados e relacionados e, daí, nasce o conceito de banco de dados. Banco de dados (Marques e Matins, 2000, p. 290) é o conjunto de dados relacionados ou relacionados com determinado assunto. Cadastro é um conjunto de registros de dados. Normalmente cadastro e banco de dados são usados como sinônimos. Ainda que haja diferenças técnicas, ambos devem ser organizados para viabilizar a recuperação e a consulta de qualquer dos dados que os componham.

O banco de dados pode ser público, privado ou de acesso público. Será público se for mantido pela Administração Pública Direta, seus órgãos e autarquias para uso de suas atribuições. É privado quando for gerido e administrado por particulares para uso próprio, sem acesso de terceiros. Banco de dados de acesso público é aquele que contém, conforme o art. 1, paragrafo único, da Lei 9.507/1997, “informações que sejam ou possam ser transmitidas a terceiros ou que não sejam de uso privado do órgão ou entidade produtora ou depositada das informações”.

O banco de dados pode ser ainda manual ou eletrônico. Será manual quando estiver organizado ou armazenado em fichas ou folhas de papel escritas manualmente, datilografadas ou impressas. Eletrônico quando os dados estiverem armazenados em sistemas de informatizados. O banco de dados em meio eletrônico (MARÇULA, 2008. P. 179) possui vantagens de gestão: armazena muitos dados, substituindo um grande volumes de papéis; localiza e atualiza os dados com rapidez; organiza em diferentes ordens; produz listas e relatórios; gera estatísticas; e permite que o tratamento seja automatizado.

Como o banco é constituído de dados, ele pode ter imagens, sons, textos, números, entre outros. O responsável pelo bando de dados é pessoa física ou jurídica, publica ou privada, que decide sobre finalidade, o conteúdo e uso do tratamento de dados.

3.1.2 Tratamento de dados

A inclusão das novas tecnologias trouxe consigo novos desafios para a sociedade, sobretudo em relação proteção à intimidade e à vida privada. Pereira (2003, p.143) comenta:

Dessa forma, os modernos computadores, com sua surpreendente capacidade de recolhimento (captura), armazenamento, tratamento e recuperação de informações, unidos à grande velocidade de transmissão de ditos dados por intermédio das distintas redes informáticas (incluídas obviamente a Internet), representam um perigo a mais para a intimidade dos indivíduos, máxime quando são utilizados para a elaboração de perfis pessoais dos usuários da Rede.

O tratamento o processamento de dados compreende a tarefa de coletar (captar), manipular (conjugar), armazenar (gravar), copiar, recuperar, apresentar (mostrar) e transmitir (comunicar) dados (MARÇULA, 2008, P. 46).

Coletar é buscar e apreender o dado; manipular consiste em conjuguar, organizar e transformar o dado; armazenar é operação de guardá-lo de forma organizada; recuperar é o procedimento de trazer o dado organizado e armazenado; mostrar é exibir o dado armazenado e transmitir é o processo de envio e recebimento de dados para os outros locais. O tratamento de dados será automatizado se utilizarem os recursos de informática em qualquer de suas etapas e não automatizados se todas as operações forem feitas física ou mecanicamente por uma pessoa.

Com os avanços tecnológicos o tratamento de dados evolui, pois a medida que se amplia o número de usuários na Internet em razão da democratização das novas técnicas aparecem. Consequentemente, como já foi citado, o resultado de toda essa evolução aumenta também a possibilidade de invasão na privacidade das pessoas. Pereira (2003) comenta sobre quantidade de informações que podem ser armazenadas e transmitidas são de tal magnitude que se exige o estabelecimento de soluções para os problemas que podem resultar da relação entre informática e intimidade.

3.1.3 Violação de dados

Existem diversas modalidades de violação de dados. Keith Darrell (2011, págs. 204-205) relaciona as principais: intrusão, divulgação accidental, violação interna, violação de equipamento portátil ou fixo, perda de cópia física e fraudes.

Na intrusão, um terceiro se infiltra e furto dados. Há divulgação accidental quando um dado é enviado para outra pessoa errada é divulgado indevidamente em meio qualquer. Configura a violação interna quando uma pessoa, com autorização de acesso, intencionalmente extrapola os limites desse consentimento.

A violação de equipamento portátil ou fixo acontece quando os dados armazenados em aparelhos portáteis ou fixo são perdidos, furtados, alterados ou apagados. A perda de cópia física é quando ocorre extravio, perda, furto ou descarte de um dado impresso. As fraudes compreende o uso indevido de dados para atacar serviços e equipamentos com o objetivo de obter vantagem ilícita ou para alterá-los deliberadamente com o fim de utilização não autorizada.

3.2 Informação

Uma modalidade especial de dados é a informação. A palavra informação vem do latim do termo *informatio*. A informação consiste em “dados dotados de relevância e propósito” (BEAL, 2004, p.12). Sempre que houver um ou mais dados que tem alguma relevância e propósito, então existirá informação. O processamento de dados procura efetuar a manipulação de dados como forma de gerar informações.

Informação é um conjunto de dados, que passaram por um tratamento e receberam um determinado significado e contexto para o sistema. Porém, apesar da relevância e propósito, necessitará de valor caso falte à interpretação.

Setzer (1999, p.3) define Informação como uma abstração informal (isto é, não pode ser formalizada através de uma teoria lógica ou matemática), que está na mente de alguém, representando algo significativo para essa pessoa. Com isso para que um dado ganhe valor de informação é preciso que o interlocutor empregue um significado:

Se a representação da informação for feita por meio de dados[...] mas, atenção, o que é armazenado na máquina não é a informação, mas a sua representação em forma de dados.[...] Por outro lado, dados, desde que inteligíveis, são sempre incorporados por alguém como informação, porque os seres humanos (adultos) buscam constantemente por significação e entendimento. [...] A informação pode ser propriedade interior de uma pessoa ou ser recebida por ela. (1999, p.3)

Por exemplo, o site Google.com possui um enorme banco de dados. Mas ao um individuo fazer uma busca qualquer, é empregado um significado a um determinado dado do enorme banco de dados que foi pesquisado, consequentemente uma informação.

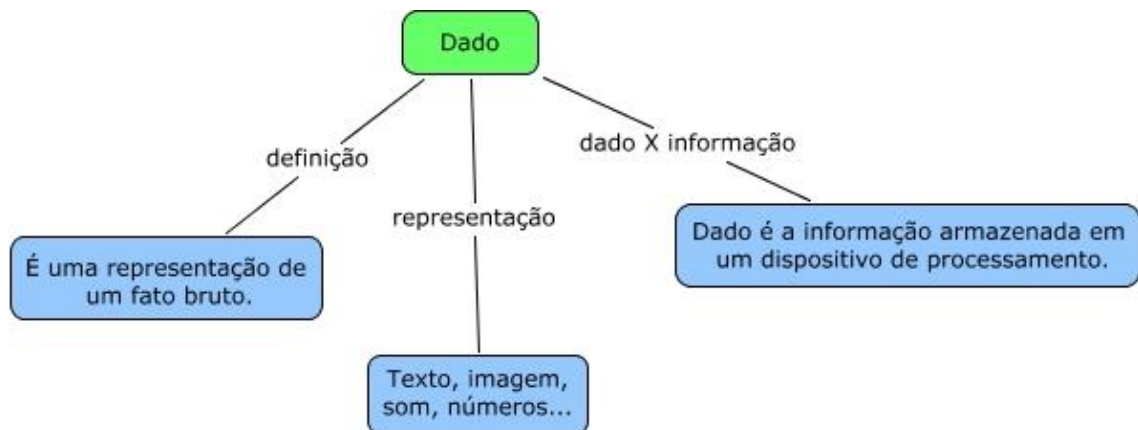
Conforme Drucker (1992), informação são dados que possuem relevância e propósito, aos quais, depois de coletados, organizados e ordenados, são atribuídos significados e contexto. Para que os dados se transformem em informação é essencial que as relações entre os vários fatos e suas implicações para os indivíduos e para a organização sejam confirmadas, tornando-se visíveis e explícitas.

Ainda de acordo com Drucker (1992) para que dados sejam convertidos em informações, é preciso perguntar do que se necessita de quem, quando e de que forma, além da certeza de que aqueles que podem prover as informações conhecem e compreendem suas responsabilidades.

Logo, informação corresponde ao registro dotados de relevância e propósito acerca de um fato, conceito, instrução, elemento ou atributo de uma pessoa. entidade ou coisa. A informação é um elemento vital para a tomada de decisões sendo o fundamento sobre o qual se assenta a tecnologia da informação, a sociedade da informação e a informática (BEAL, 2004, p.13).

Segundo Nonaka e Takeuchi (1997), a informação é um fluxo de mensagens e por meio dela não só se extrai como também se constrói o conhecimento. Sveiby (1998) destaca que o valor não está na informação armazenada, mas na criação de conhecimento de que ela pode fazer parte. Informação é a disposição dos dados de tal forma que possuam sentido, criando padrões e ativando significados na mente das pessoas como esquematizado na Figura 1.

Figura 1: Significação do dado



Fonte: Produzido pela autora

Pierre Catala (1983) explica que o dado pessoal mesmo que não tenha sido gerado pelo indivíduo, mas se o apresentar relação e identificação com a informação se torna passível de tutela jurídica:

Mesmo que a pessoa em questão não seja a 'autora' da informação, no sentido de sua concepção, ela é a titular legítima de seus elementos. Seu vínculo com o indivíduo é por demais estreito para que pudesse ser de outra forma. Quando o objeto dos dados é um sujeito de direito, a informação é um atributo da personalidade. (CATALA, 1983, p. 20)

Segundo esclarece Stair (1998, p.4), informação "é um conjunto de fatos organizados de tal forma que adquirem valor adicional além do valor do fato em si". Daí a grande quantidade de dados que as pessoas são, diariamente, solicitadas a fornecer, pois quanto maior o número de dados pessoais, melhor a informação obtida e conseqüentemente mais valiosa. Por sua vez, Stair completa definindo dados como "os fatos em sua forma primária, como por exemplo, o nome de um empregado e o número de horas trabalhadas em uma semana, números de peças em estoque, ou pedidos de venda" (1998, p.4). Concluindo que os dados apenas terão valor se organizados ou arranjados de uma maneira significativa, a fim de se tornarem uma informação.

3.2.1 Tecnologia da informação

O termo tecno, que compõem a palavra tecnologia, vem do grego teknè, que significa arte. Técnica é uma arte prática, de saber fazer humano, por isso, para "os

gregos, todo o ato humano é *teknè* e todo *teknè* tem por característica fazer nascer uma obra" (LEMOS, 2010, P. 27). Essa ideia de fazer nascer uma obra, de dominar a arte prática do saber-fazer está presente na noção de tecnologia da informação.

Tecnologia da informação (ou tecnologia da informação e comunicação) é a prática de equipamentos de Informática ou de telecomunicações para gravar, recuperar, transmitir e manipular dados.

3.2.2 Sociedade da informação

Diante das mudanças do mundo e na sociedade provocadas pelo avanço proporcionado pela tecnologia da informação, Jacques Delors em 1993, durante o Conselho Europeu de Copenhague⁹, cunhou a expressão sociedade da informação.

Sociedade da informação é (BEAL, 2004, p.22), uma nova forma de organização social política e econômica que recorre ao intensivo uso da tecnologia da informação para coleta produção processamento transmissão e armazenamento de informações.

3.3 Dados pessoais

Os dados pessoais são conceituados de forma clara pelo o Professor Warcks, os definindo o termo como:

Dados pessoais consistem nos fatos, informações, ou opiniões que dizem respeito a um indivíduo e que seria razoável esperar que ele considerasse como íntimo ou compassivo e, portanto, querer reter ou, pelo menos, restringir a sua coleta, utilização ou circulação.¹⁰ (p. 26, 1989, Tradução nossa)

Dessa forma, pode-se dizer que dados pessoais são qualquer informação referente a uma pessoa singular identificável a partir dos dados. Danilo Donela (2006, p. 133) elucida que, a informação pessoal difere de outras informações por possuir um vínculo objetivo com a pessoa, isto é, por manifestar-se aspectos que lhe

⁹Conselho Europeu de Copenhaga — 21-22 de Junho de 1993. Disponível em: <<http://www.consilium.europa.eu/pt/european-council/conclusions/pdf-1993-2003/conclus%C3%B5es-da-presid%C3%A2ncia---copenhaga,-21-22-de-junho-de-1993/>> Acesso em: jun. de 2017

¹⁰ "Personal information" consists of those facts, communications, or opinions which relate to the individual and which it would be reasonable to expect him to regard as intimate or sensitive and therefore to want to withhold or at least to restrict their collection, use, or circulation.

dizem respeito. Dessa forma, tais conceitos deixam clara a necessidade da tutela jurídica, por serem os dados pessoais um objeto de uma única pessoa, sendo um bem, mesmo que intangível. É primordial perceber que tal tutela dirige a proteção da pessoa e da personalidade das informações e não apenas dos dados *per se*.

3.3.1 Dados anônimos

É possível também que os dados se refiram a pessoas indeterminadas, que são os dados anônimos, que nessa conjuntura são considerados apenas dados. Sem nenhuma identificação de algum indivíduo, normalmente são utilizados apenas para fins estatísticos.

Sendo assim, ao adquirirem a característica de dados anônimos, esses dados não estão mais sujeitos a tutela jurídica, pois, não são passíveis de identificação. E a proteção de dados pessoais só envolve os dados identificáveis a alguma determinada pessoa.

3.3.2 Dados sensíveis

Dados sensíveis são aqueles que além de identificarem a pessoa, revelam elementos mais profundos de sua personalidade, como sua posição política, ideológica, religiosa, sexual, além de trazerem, entre outros aspectos, informações relacionadas à saúde, origem racial, étnica e genética.

O professor Doneda (2006, p. 163), comenta sobre a importância da proteção destes dados, já que a violação de dados sensíveis é muito mais prejudicial para a pessoa em causa, podendo gerar danos mais intensos à sua personalidade. Outra abordagem envolve a consideração de que o mau uso de dados sensíveis pode trazer maiores possibilidades de discriminação do indivíduo.

Os dados sensíveis dizem a respeito, por exemplo, à origem racial ou étnica da pessoa, às suas opiniões políticas, filosóficas ou religiosas, à sua saúde e a opção sexual. É justamente por essa razão que eles possuem um potencial de maior de causar ofensa a direitos fundamentais, não apenas à intimidade mas, especialmente, à igualdade e a não discriminação.

Em situações concretas, um dado pessoal aparentemente não sensível pode se torna sensível e apresentar-se fator de discriminação, como nos casos em que um nome revela origem racial ou étnica, Tatiana Vieira destaca que:

O tratamento de dados sensíveis exige a adoção de medidas e procedimentos mais rigorosos de segurança, tais com autenticação de quem acesso sistema informático; o acesso restrito às instalações físicas, em que o sistema informático se localiza; a destruição automática de dados após o cumprimento de suas finalidades; uso criptografia para cifragem do conteúdo dentre outros. (2007, p. 256)

Os dados pessoais, em particular os sensíveis são aqueles que demandam especial proteção, principalmente perante as novas tecnologias, das diversas redes sociais e da Internet . A deriva nº 95/46 da União Europeia estabelece em seu artigo 8º a regra geral de proibição de tratamentos de dados sensíveis.

3.3.3 *Big Data*

Esse termo começou a ganhar destaque a partir dos anos 2000, com Doug Laney¹¹, um analista que formulou a definição de Big Data. Akerkar (2014) conceitua:

Big Data refere-se a conjuntos de dados, cujo tamanho está além das capacidades da tecnologia de banco de dados atual. É um campo emergente onde a tecnologia inovadora oferece alternativas para resolver os problemas inerentes que aparecem quando se trabalha com dados massivos, oferecendo novas maneiras de reutilizar e extrair valor a partir de informações.¹² (p. 104, Tradução nossa)

Sathi apresenta alguns tipos e características do Big data:

Existem duas fontes comuns de dados agrupados sob a bandeira do big data. A primeira são os dados internos (dados estruturados, não estruturados ou semiestruturados) da organização que, graças à automação e acesso estão sendo cada vez mais compartilhados. A segunda são os dados de fora da organização, como as informações disponíveis em sites de mídia social, literatura do produto distribuído livremente pelos concorrentes, hierarquias organizacionais dos clientes corporativos, dicas úteis

¹¹ O analista do Gartner, Doug Laney, introduziu o conceito de 3Vs em uma publicação de pesquisa MetaGroup de 2001, gerenciamento de dados 3D: controle de volume, variedade e velocidade de dados. Disponível em: <<https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf>> Acesso em: 03 de outubro de 2017.

¹² *The term Big Data refers to data sets the size of which is beyond the capabilities of current database technology. It is an emerging field where innovative technology offers alternatives to solve the inherent problems that arise when working with massive data, offering new ways to reuse and extract value from information.*

disponíveis a partir de terceiros e reclamações de clientes postados em sites de regulamentação¹³ (p. 16, 2012, Tradução nossa)

Big Data vem chamando atenção pela acelerada escala em que volumes cada vez maiores de dados são criados pela sociedade. Por isso cada vez mais se destaca, em um relatório o McKinsey Global Institute colabora com a compressão do tema:

Os dados gerados são rapidamente crescente, refletindo a adoção crescente de smartphones e outras aplicações. Este domínio é um viveiro de inovação que poderia transformar as organizações e as vidas de indivíduos, potencialmente, criar uma quantidade significativa de excedente para os consumidores.¹⁴ (p. 38, 2011, Tradução nossa)

No Brasil, um dos influentes percussores do Big Data é Cezar Taurion (2013, p.30), define o termo com uma formula simples, Big Data = volume + variedade + velocidade + veracidade + valor. Técnica essa que emprega todos esses elementos no tratamento de dados, por isso tão importante e evidente nos últimos tempos.

Para uma melhor compressão dos cinco V's apresentados por Taurion em sua obra Big Data de 2013 se faz necessário pontuar cada um deles:

- Volume parece ficar claro, pois o Big Data como já dito em conceitos é um enorme volume de dados. São gerados petabytes de dados a cada dia, estima-se que este volume dobre a cada 18 meses;
- Variedade, pois estes dados podem vir de sistemas estruturados e não estruturados (maioria), que são gerados por redes sociais (Facebook, Twitter, YouTube e outros), e-mails, visitas ou cadastros em sites de compras, mensagens instantâneas, sensores, câmeras de vídeo, etc;
- Velocidade, porque muitas vezes precisamos agir praticamente em tempo real sobre este imenso volume de dados;

¹³ So, what is Big Data? There are two common sources of data grouped under the banner of Big Data. First, we have a fair amount of data within the corporation that, thanks to automation and access, is increasingly shared. This includes emails, mainframe logs, blogs, Adobe PDF documents, business process events, and any other structured, unstructured, or semi-structured data available inside the organization. Second, we are seeing a lot more data outside the organization— some available publicly free of cost, some based on paid subscription, and the rest available selectively for specific business partners or customers. This includes information available on social media sites, product literature freely distributed by competitors, corporate customers' organization hierarchies, helpful hints available from third parties, and customer complaints posted on regulatory sites.

¹⁴ The data generated are growing quickly, reflecting the burgeoning adoption of smartphones and other applications. This domain is a hotbed of innovation that could transform organizations and the lives of individuals, potentially creating a significant amount of surplus for consumers.

- Veracidade, porque precisamos ter certeza que os dados fazem sentido e são autênticos;
- E por fim o Valor, porque é absolutamente necessário para organização que implementa projetos de Big Data obtenha retorno destes investimentos. Pois, só faz sentido se o valor da análise dos dados compensar o custo de sua coleta, armazenamento e processamento.

Ainda existe a necessidade de destacar que a computação em nuvem é um impulsionador do Big Data, pois através dessa tecnologia pode-se armazenar imensos volumes de dados, além da característica de elasticidade das nuvens permitem que acionemos servidores virtuais sob demanda, apenas no momento de tratar estes dados. Existem ainda diversas questões legais a serem resolvidas sobre o tema.

3.3.4 *Small Data*

Já não é novidade a rapidez com que as coisas se renovam e se transformam, seja por necessidade ou otimização. O small data veio para auxiliar e não substituir o big data. Small Data basicamente conecta as pessoas com as oportunidades, é um pequeno conjunto de dados, localizados em equipamentos individuais e utilizados em decisões rotineiras.

O conceito apresentado pelo site Techopedia (2016):

Small Data, se conectam com as pessoas com oportunas, insights significativos (derivados de grandes dados e/ou fontes de "locais"), organizado e armazenados - muitas vezes visualmente - para ser acessível, compreensível e acionável para as tarefas diárias.¹⁵ (Tradução nossa)

Enquanto o *Big Data* apresenta os cinco Vs, o *Small Data* tem palavras chave como:

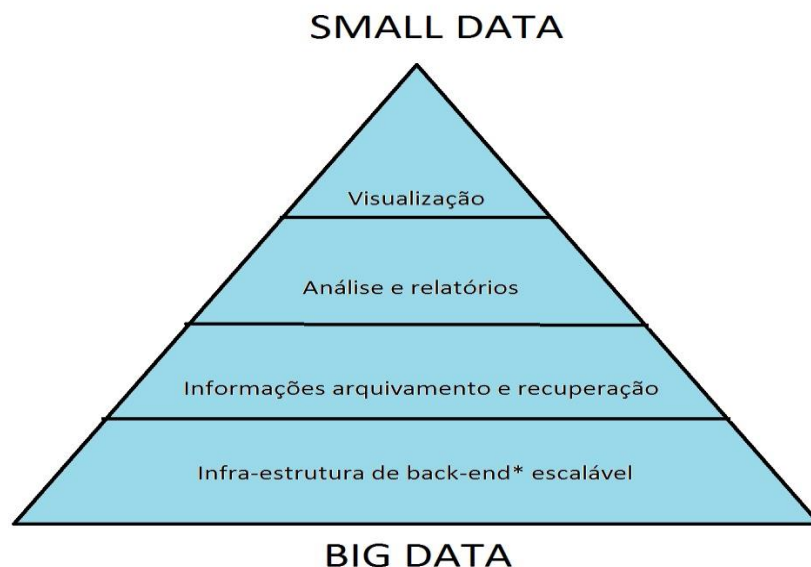
- Conectar (connect);

¹⁵ Small data connects people with timely, meaningful insights (derived from big data and/or "local" sources), organized and packaged – often visually – to be accessible, understandable, and actionable for everyday tasks. Disponível em: <<https://www.techopedia.com/definition/29539/small-data>> Acesso em: 03 de outubro de 2017.

- Organizar (organize);
- Armazenar (package);
- Valor (value).

Enquanto o Big Data se preocupa em achar correlações em grandes volumes de dados. O Small Data está atento as causas e os motivos que estão por trás das coisas. Valorizando a interação pessoal, basicamente com aplicação em informações acessíveis, compreensíveis e aplicáveis, e com foco no usuário final, o que eles precisam, e como eles podem decidir melhor. Ao observar a figura 2, podemos ter um melhor entendimento:

Figura 2: Comparação entre o *Big Data* e o *Small Data*



Fonte: Adaptado de D8A GROUP¹⁶

Ao analisar a pirâmide a base é o grande volume de dados extraídos pelo Big Data, através do sistema back-end¹⁷, formando a base da pirâmide. Enquanto as empresas que usam Small data se concentram na experiência do usuário final com os aplicativos e produtos de visualização que parecem ser mais simples do que

¹⁶ Figura traduzida.

Fonte: <<http://blog.d8a.com/post/27473432923/what-is-big-data-what-is-small-data>>

¹⁷ O back-end de um sistema é a parte que você como usuário não consegue ver e nem usar. Mas ela é fundamental para a existência de um site ou sistema. Questões sobre performance, persistência de dados, são atividades rotineiras de um programador back-end. back-end utiliza diversas linguagens de programação, como por exemplo, Java, C#, Ruby, Python, PHP e muitas outras. Disponível em: <<http://aprendizweb.com.br/front-end-e-back-end/>> Acesso em: 03 de outubro de 2017.

realmente são. As empresas que costumam empregar pouco trabalho computacional, se eles se estendem por todo o caminho até a base da pirâmide, ou parar em algum lugar no meio, caso já tenha realizado o objetivo.

4 PRINCÍPIOS PARA A PROTEÇÃO DE DADOS PESSOAIS

O desenvolvimento nas duas ultima décadas da pratica jurídica brasileira, no âmbito de iniciativas legais e infralegais, sugerem uma evolução do conceito privacidade também entre nós, inclusive com a aplicação de diversos princípios relacionados á proteção de dados pessoais consolidados na doutrina internacional.

4.1 Os direitos subjetivos do titular dos dados pessoais

O pressuposto de que o indivíduo deve ter o poder de controlar o fluxo dos seus dados pessoais requer que lhe sejam atribuídos determinados direitos subjetivos em face dos responsáveis pelo controle dos bancos de dados. Esses direitos presentes na maioria das legislações sobre o tema podem ser resumidos aos seguintes: direito geral á informação; direito de acesso; direito de notificação; direito de retificação cancelamento e bloqueio dos dados; e; direito de não se ficar sujeito a uma decisão individual automatizada.

O direito geral de informação consiste no direito o que as pessoas têm de conhecer sobre a existência dos bancos de dados, bem como seus objetivos e de seu conteúdo. Para que o indivíduo possa proteger a sua personalidade, é preciso que todo o processo de tratamento de dados pessoais seja transparente. Assim, conforme a Lei de Proteção de Dados Pessoais de Portugal, a Lei n. 67/98, o direito à informação consiste no direito do indivíduo cujos dados são coletados de conhecer a identidade do responsável pelo tratamento o objetivo do tratamento, e os destinatários dos dados em caso de transferência¹⁸. Ademais, o indivíduo deve ser informado a respeito dos quais são os seus direitos e como ele pode exercer em cada fase do tratamento dos seus dados pessoais.

De acordo com Murillo (1990), direito de acesso refere-se ao direito do indivíduo para receber mmpa informação acerca dos dados registrados sobre ele, sempre que requisitar. Essa faculdade compreende o conhecimento sobre os dados armazenados, incluindo informações acerca de sua origem; sobre os organismos receptores das informações transmitidas ou a sua categoria; e sobre o objetivo do armazenamento. A frequência desse acesso varia de acordo com as diversas

¹⁸ Lei de Proteção de Dados Pessoais de Portugal, art. 10 – (Lei n. 67/98)

legislações, assim como a sua gratuidade ou onerosidade. Entende-se que, para a garantia da efetividade do referido direito, seria fundamental garantia a gratuidade do acesso a essas informações, conforme estabelece, por exemplo, a Lei da Federação de Proteção de Dados Alemã (BDSG)¹⁹, em seu art. 19.

O direito de acesso compreende também o direito do indivíduo conhecer, na hipótese da existência de um conjunto de banco de dados, em qual banco de dados estão armazenados as suas informações. Nesse caso, pode o cidadão procurar qualquer um desses bancos, que terá a obrigação de encaminhar sua solicitação ao organismo responsável pelo armazenamento, bem como comunicar a informação ao cidadão.

O direito de notificação está relacionado aos direitos anteriores e surge para o indivíduo sempre quando os seus dados foram coletados sem seu conhecimento. Nessa hipótese, conforme o Federal Data Protection Act (BDSG), deve um indivíduo ser informado sobre o armazenamento, à identidade do responsável pelo banco de dados e o objetivo do tratamento²⁰. O indivíduo deve ser notificado também em caso de transferência de seus dados, devendo constar na notificação os organismos receptores. Os direitos de retificação, cancelamento e bloqueio dos dados visando assegurar a princípio da qualidade dos dados pessoais, de modo a corrigir luz em caso de equívoco, cancelá-los, caso estejam obsoletos ou tenham sido indevidamente armazenados, e bloqueá-los, na hipótese de o cancelamento não se possível fatidicamente ou não ser permitido por lei²¹. Os dados devem ser bloqueados também na hipótese de haver uma controvérsia sobre a sua veracidade e não houver sido apresentado prova para confirmá-la.

¹⁹ ALEMANHA. Federal Data Protection Act (BDSG) In the version promulgated on 14 January 2003. Federal Law Gazette I, p. 66. Last amended by Article 1 of the Act of 14 August 2009 (Federal Law Gazette I, p. 2814), in force from 1 September 2009. Disponível em: <<http://dzlp.mk/sites/default/files/Dokument/EU%20zakoni%20zzlp/GERMANY.pdf>>. Acesso em: 03 de outubro de 2017.

²⁰ "(1) The collection, processing and use of personal data shall be lawful only if permitted or ordered by this Act or other law, or if the data subject has provided consent." (ALEMANHA, 2009, p. 8)

²¹ "Personal data shall be collected, processed and used, and data processing systems shall be chosen and organized in accordance with the aim of collecting, processing and using as little personal data as possible. In particular, personal data shall be rendered anonymous or aliased as allowed by the purpose for which they are collected and/or further processed, and as far as the effort required is not disproportionate to the desired purpose of protection." (ALEMANHA, 2009, p. 7).

Em caso de correção, bloqueio ou cancelamento dos dados, é direito do indivíduo que todos os organismos que receberam por transferência os seus dados sejam identificados para tomarem as devidas providências. Nesse sentido, tem-se, por exemplo, a Lei da Federação de Proteção de Dados Portuguesa em seu art. 11 e a Lei da Federação de Proteção de Dados Alemã, em seu art. 20.

Previsto no art. 15, Diretiva Europeia 95/46/CE, o direito de não se ficar sujeita a uma decisão individual automatizada consiste no direito do cidadão de não ficar submetida a decisões que influenciam significativamente a sua posição jurídica, tomadas exclusivamente com base no tratamento automatizado de dados. Deste modo, tal regra constitui uma proibição geral referente a decisões automatizadas, podendo ocorrer apenas em duas hipóteses, conforme a Diretiva: desde que existam medidas adequadas para que garantam a representação e expressão do titular dos dados para a sua defesa o que ocorreu no âmbito da celebração ou a execução de contratos.

Tal o direito consiste, na realidade, em uma regra de justiça, que visa assegurar a possibilidade de Defesa do titular e a mínima participação do titular em um processo decisão tomada com base em seus dados e que afetará de forma significativa suas oportunidades de vida.

4.2 Princípios de proteção dos dados pessoais

Ao longo do desenvolvimento do conceito de privacidade proteção de dados pessoais, estabeleceu-se, por meio de instrumentos internacionais e transnacionais.

Conforme Bennett (1992, p.95), um consenso em torno de um quadro básico de princípios que devem nortear a atividade de tratamento de dados. Esses princípios têm como finalidade limitações ao tratamento de dados, bem como atribuir poder ao indivíduo para que esse possa controlar o fluxo de seus dados. Os dados pessoais e sensíveis são subordinados a uma principiologia própria que permeia o ordenamento jurídico nacional e gerando diferentes tipos de cadastros, especialmente os públicos e os de caráter publico, inclusive os acessíveis pelas diversas redes de informática de caráter publico, nos termos do art. 5 LXXII, a, da Constituição e art. 19, paragrafo único, Lei do Habeas Data (Lei 9.507/1997).

O panorama das leis estrangeiras descreve vários princípios inclinados a proteção dos dados pessoais. São princípios gerais de direito inerentes aos dados pessoais. Muitos deles estão expressamente previstos em leis esparsas, tais como o Código Civil, Código Penal, Código Defesa do Consumidor e nas Leis 9.507 de 1997 e 12.414 de 2011. Também dos direitos fundamentais insertos da Constituição da República é possível extrair tais princípios.

Serão apresentados os princípios básicos de proteção de dados pessoais, com base nas legislações citadas.

4.2.1 Princípio da finalidade

Um princípio fundamental que todas as atividades de processamento de dados devem seguir o princípio da finalidade, que indica a qual a relação necessária que deve existir entre o uso dos dados pessoais e a finalidade comunicado aos interessados quanto à coleta dos dados. Esse princípio é essencial para se limitar o acesso de terceiro dos bancos de dados. Segundo Doneda (2006, p.216), ele também serve como parâmetro para julgar se determinado uso de dados pessoais é adequado e razoável, de acordo com a finalidade informada no primeiro momento ao interessado.

Paula Ribeiro (2010, p. 790) assevera que o conceito de finalidade incompatível não possui um significado muito claro, pelo que, usando um argumento a contrário, poderia levar uma considerável ampliação para o uso de dados pessoais. Significa dizer, os dados só não poderiam ser usados para fins incompatíveis, avessos e contrários a sua finalidade para qual tenham sido obtidos. As possibilidades de uso seriam, assim, dimensionadas pelo universo restante, muito mais amplo, portanto. A autora ainda discorre que, os dados pessoais só devem ser coletados, tratados e para atender a finalidade explícita e determinada, devidamente informada ao titular dos dados.

Por fim, esse princípio exige que o responsável pelo tratamento de dados, estabeleça de que forma expressa e limitada a finalidade do tratamento de dados, sob a pena de se considerar ilegítimo o tratamento realizado com base em finalidades amplas e genéricas. Nada obstante, o tratamento posterior para fins

históricos, estatísticos ou científicos não é considerado incompatível, desde que se estabeleçam garantias adequadas.

4.2.2 Princípio da transparência

O princípio da Transparência também chamado de princípio da publicidade exige que a existência de um banco de dados seja de conhecimento público. Ele reafirma o preceito democrático, segundo o qual não pode existir bancos de dados sigilosos, e baseia-se na ideia que a transparência é uma das principais formas de combate aos abusos.

Com base nesse princípio, surge para os detentores dos bancos de dados o dever de publicar seu nome, sede e conteúdo, em registros públicos, diários oficiais ou meios de grande circulação, sobre pena de ineficácia desse direito. Bennett (1992, p. 156) cita que em alguns países, exigem autorização estatal prévia ou notificação aos órgãos supervisores como pressuposto para funcionamento desses bancos de dados. Percebe-se que o princípio da Transparência é uma condição essencial de *accountability* dos bancos de dados.

4.2.3 Princípio do consentimento

Para possibilitar o controle do titular acerca dos seus dados, outro princípio relevante é o princípio do consentimento. Afinal, o exercício de liberdade de controle dos dados pessoais baseia-se no consentimento do titular, que pode determinar o maior nível de proteção ou maior fluxo dos seus dados. Segundo esse princípio o consentimento deve ser livre, específico e informado, e apenas em situações (previstas legalmente) justificam o processamento de dados sem o prévio consentimento do titular. Permitisse ao interessado exercer maior nível de proteção ou dar um maior fluxo aos seus dados.

De acordo com a Diretiva da União Europeia, nº 95/46/CE de 1995, o consentimento se trata de: "qualquer manifestação, livre, específica e informada, pela qual a pessoa em causa aceita que os dados pessoais que lhe digam respeito sejam objeto de tratamento". O direito fundamental á liberdade, inserto no art. 5º, caput, da Constituição, nasce da perspectiva da pessoa humana como ser em busca

da autorealização, responsável pela escolha dos meios aptos para realizar suas potencialidades. A liberdade não deve ser apenas formal, mas sim afetiva. Deve permitir que a pessoa faça suas próprias escolhas e bem conduza os destinos de sua vida. Além disso, o conteúdo negativo da liberdade individual referente à autonomia, à garantia contra ingerências externas, também deve ser efetivo.

Não há, contudo, uma ordem absoluta outorgada ao consentimento. Não é apenas a vontade do titular que regula a proteção de dados pessoais. Estando em causa e valores fundamentais do Estado Democrático de Direito, como a dignidade da pessoa humana, a ordem constitucional cuida de estabelecer níveis de proteção necessários conforme a categoria e a natureza dos dados. Nada obstante, conforme Faria (2010, p.792) existe uma importante relação entre o consentimento e a licitude da coleta e do tratamento dos dados pessoais que poderá ser afastada ou derogada apenas nos casos particulares conforme a lei.

Stefano Rodotà (2008, p. 89) apresenta crítica importante sobre a questão. Observa que em se tratando de serviços essenciais ou importantes - como em casos diversos serviços informáticos e telemáticos -, não ocorre à liberdade do consentimento, que acaba sempre condicionado. O condicionamento deriva do fato de que a possibilidade de usufruir de serviços depende do fornecimento de diversas informações pessoais pelo usuário que forçosamente em fornecê-las. Ele ainda conclui que há uma forte pressão exercida pelos gestores das novas mídias interativas, por evidentes razões econômicas, sobre usuários para que autorizem a elaboração dos perfis pessoais ou familiares baseados nas informações coletadas por fornecimento dos serviços.

As exceções o consentimento passam: pela necessidade a execução de um contrato no qual o interessado seja parte; por cumprimento e a obrigação legal que esteja sujeita ao responsável pelo tratamento de dados; se houver necessidade para proteção de interesses vitais do titular dos dados; se fizer parte de missão de interesse público o exercício de autoridade pública parte responsáveis pelo tratamento dos dados; e se for necessário para perseguir interesses legítimos do responsável pelo tratamento dos dados. O princípio do consentimento também vem expresso na Diretiva 95/46/CE.

4.2.4 Princípio da lealdade ou boa-fé

Outro princípio relevante é o princípio da lealdade ou da boa-fé, extraído da Diretiva 95/46/CE em seu art. 6º. Ele se refere à exigência de que os dados constantes de um banco de dados sejam objeto de um tratamento leal e lícito, sejam adequados pertinentes e não excessivos em relação à finalidade declarada, além de serem objetivos, exatos e atualizados. Onde os dados pessoais somente devem ser recolhidos com o conhecimento do indivíduo e em circunstâncias nas quais ele possa se opor à coleta de seus dados.

O princípio é de grande importância e alcance prático, tendo repercussão direta sobre a prática de data mining largamente utilizada na Internet. Conforme Zanon (2012) esse princípio, a utilização de *cookies*, *spywares*, *keyloggers* ou outros expedientes utilizados para rastrear os padrões e comportamento dos usuários que navega na rede são ilícitas, salvo se levados ao conhecimento do internauta conferindo-lhe oportunidade e meios para desabilitar os coletores de dados.

Rodotá (2008), sustenta que o conjunto de tutelas oferecidas ao cidadão tende a se estender dos dados em saída àqueles em entrada. Assim, atribui especial importância ao direito de não saber, que concretamente se traduz no direito de não receber comunicações indesejadas ou para as quais não foi dado consentimento preventivo. O direito de não saber opor-se-ia, assim, a prática de *spamming*²².

Tal princípio enseja cautela na formação do banco de dados, assim como a demanda a sua constante atualização, de forma a impedir que os dados contidos resultem ultrapassados com o passar do tempo. A atividade do princípio da boa fé é fundamental a garantia dos direitos de acesso retificação e cancelamento dos dados.

²² Termo de origem inglesa cujo significado designa uma mensagem eletrônica recebida, mas não solicitada pelo usuário. O conteúdo de um spam é normalmente uma mensagem publicitária que tem o objetivo de divulgar os serviços ou produtos de alguma empresa a uma grande massa de usuários de e-mail.

4.2.5 Princípio da segurança física e lógica

O princípio da segurança física e lógica refere-se à exigência básica de que qualquer banco de dados pessoais esteja protegido contra extravios, destruições, modificações e desvios não autorizados pelos interessados.

De acordo com Moraes (2010) pode-se definir Segurança da Informação como um processo de proteger informações do mau uso sendo ele intencional ou não, sendo por pessoas internas ou externas à organização. Ress (2011) segue a mesma linha afirmando que a segurança tem como objetivo garantir a confidencialidade, integridade e disponibilidade dos elementos no qual os dados utilizam.

Segundo Comer:

A segurança implica em proteção incluindo a garantia da integridade dos dados, impedimento de acesso não-autorizado de recursos computacionais, impedimento de escutas ou grampos e impedimento de interrupção do serviço. Naturalmente, assim como nenhuma propriedade física é absolutamente segura contra crime, nenhuma rede é completamente segura. As organizações se esforçam para proteger as redes pelo mesmo motivo pelo qual se esforçam para proteger prédios e escritórios: medidas de segurança podem desencorajar o crime, tornando-o significativamente mais fácil. (COMER, 2006, p. 359)

A segurança é um fator determinante para o sucesso ou fracasso de uma organização, este tema é cada vez mais discutido no mercado da tecnologia, tendo a crescente necessidade de proteção dos dados armazenados e transmitidos. Isso se afirma pelos constantes estudos. Para Comer (2006, p.359), “Fornecer segurança para a informação exige proteger os recursos físicos e abstratos”. Para Soares, et al (1995, p.448) “o termo segurança é usado com o significado de minimizar a vulnerabilidade de bens (qualquer coisa de valor) e recursos”. A segurança dos dados pessoais deve ser física e lógica, contra parcial ou total destruição, perda ou alteração, ainda que incidental. Também compreende o acesso, a invasão ou a divulgação por terceiro não autorizado.

Conforme Vieira (2007, p.294) “protegendo-as do acesso não autorizado (comprometimento do sigilo), da alteração (comprometimento da integridade) e da destruição (comprometimento da disponibilidade, além da exploração de outras vulnerabilidades”. Pelo princípio da segurança, o responsável

pelo armazenamento de dados pessoais deve adotar medidas técnicas e administrativas que garantam a segurança de tais informações.

4.2.6 Princípio da responsabilidade

Por fim um importante princípio da matéria de proteção de dados pessoais é o princípio da responsabilidade, que visa assegurar a reparação adequada integral dos danos materiais e morais causados ao indivíduo em razão da violação de seu direito à privacidade decorrente ao tratamento dos seus dados pessoais.

Nos termos da Diretiva 95/46/CE, art.23, qualquer pessoa que sofra um prejuízo devido ao tratamento ilícito de dados, conforme nela estabelecido, ou em razão de qualquer ato proscrito pela Lei Nacional do Estado-Membro tem direito de obter do responsável pelo tratamento respectivo reparação. Admite, contudo a norma comunitária exoneração total ou parcial de responsabilidade do responsável pelo tratamento dos dados pessoais se provar que o fato que causou o dano não lhe é imputável.

Nota-se assim que neste aspecto a Diretiva europeia é conservadora. Com efeito, embora que possa sustentar que tenha estabelecido a responsabilidade objetiva do responsável pelo tratamento dos dados pessoais (já que não menciona a necessidade de conduta culposa ou dolosa para obrigação de indenizar), a Diretiva por outro lado, concede considerável abertura para a exoneração de sua responsabilidade. Responsável pelo tratamento de dados eximir-se-á, total, ou parcialmente, de responsabilidades sempre que o fato causador do dano não lhe foi imputado como nas hipóteses de culpa de terceiro, situação muito comum em ambientes online.

Neste particular, o Código Italiano em matéria de tratamento de dados pessoais é mais avançado. Em seu art. 15, a Lei italiana classifica o tratamento de dados pessoais como atividade perigosa, ao remeter a obrigação de indenizar ao artigo 2.050 do Código Civil italiano²³ que dispõe sobre a responsabilidade por

²³ No Código Civil Italiano, art. 2050 que dispõe: “Aquele que emprega na atividade produtiva ou na vida privada meios que são fonte de perigo aceita com isso a eventualidade de ocasionar danos aos outros, deve por consequência assumir o risco de dever-lhe ressarcir também se não lhe tenha ocasionado por culpa”

atividades potencialmente perigosas. Trata-se de disposição legal semelhante ao que dispõe o Código Civil brasileiro em seu art. 927, parágrafo único²⁴.

4.2.7 Princípio da proibição de tratamento de dados sensíveis

Constitui objetivo da Diretiva 95/46/CE, em seu artigo 1º, assegurar às pessoas singulares a proteção das liberdades e dos seus direitos fundamentais. Dentro desse propósito, assume especial relevância o princípio que rege o tratamento dos dados sensíveis. Assim o anuncia expressamente o artigo 8º da Diretiva 95/46/CE: "Os Estados-Membros proibirão o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual". São considerados dados sensíveis dos elementos de informação que podem dar origem a tratamentos desiguais ou discriminatórios, além de contenderem em grande parte das vezes com a intimidade do seu titular. Nesse sentido, o princípio é de proibição da coleta e tratamento dessa categoria de dados. As informações genéticas tem recebido especial atenção e proteção, decorrente de fato que estão relacionadas a própria estrutura da pessoa. Não são modificáveis pela vontade do titular (como opiniões e convicções pessoais) e não podem ser removidas ou esquecidas (a exemplo de comportamentos passados). Exatamente por seu caráter estrutural e permanente, as informações genéticas fornecem o perfil mais definido da pessoa, e estão muitas vezes, na base de ações discriminatórias, elevando à necessidade de fundamental proteção sobre essa espécie de dados pessoais.

Vera Lúcia Raposo (2010) comenta que o *Terrorist Identification Data-Base Act*, editado nos Estados Unidos da América em 2003, impôs a colheita obrigatória de DNA no âmbito de Investigações e repressões atividades terroristas (a recusa a carreta sanção pecuniária pesadíssima). Diante do fato, observa que os critérios comentam o possível em creme de preconceitos racistas, porquanto a grande maioria dos envolvidos são de ascendência árabe.

²⁴ CC - Lei nº 10.406 de 10 de Janeiro de 2002 - Código Civil.

Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo. Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.

O direito a não saber também se faz presente em tratamentos de dados genéticos. Conforme a doutrina, se é muitos de nós gostaríamos de conhecer aquilo que amanhã nos reserva, outros preferem não saber quando morreram e a qual causa da morte radicando esta opção ainda na autonomia pessoal mais propriamente no direito à proteção dos dados pessoais. Neste particular, Vera Lucia (2010, p. 967) concluiu que nos casos de exame de DNA há que se atentar que poderão implicar para o paciente conhecimento de informações sobre seu estado de saúde presente ou futuro que eventualmente desejar e não saber.

A proibição de tratamento cidade sensíveis, porém não é absoluta comportando exceções. Dados relativos ao comportamento criminal do cidadão normalmente recebem tratamento disciplinar mais rigoroso. O tratamento dessa categoria de dados fica restrita aos órgãos públicos competência específica, com procedimentos e medidas adequadas de proteção e segurança.

Catarina Sarmiento e Castro (2015, p. 94) advertem que o uso de dados pessoais para fim policiais apenas deverá ter o lugar de forma pontual, quando esteja em causa prevenir um perigo concreto ou reprimiu infração penal determinada, devendo limitar-se aos dados necessários. Não podem servir para estabelecer mecanismos de controle geral e contínuo, vigiando qualquer um o tempo todo. Acrescenta que eventuais partilhas de dados de leitos por serviços policiais dos Estados devem ocorrer apenas entre autoridades policiais e não entre quaisquer outras.

De uma maneira geral, os países europeus ao transporem as normas comunitárias para seus respectivos direitos nacionais tem estabelecido três hipóteses e as ações ao dever de proibição do tratamento de dados sensíveis:

(a) mediante o consentimento expresso do titular dos dados; (b) através de autorização legal em casa justificados e com garantia de não discriminação; (c) para processamento dos dados para fins estatísticos e históricos desde que tomadas as medidas para torná-los não individualmente identificáveis. (CANOTILHO, 2007, p. 577)

De toda forma, em se tratando de dados sensíveis, o consentimento é sempre peça fundamental, exigindo-se que seja manifestado de modo expresso e específico pelo titular dos dados pessoais. Saliente-se que a manifestação do titular deve se dar mediante o consentimento informado.

Trata-se de isentar a pessoa de graves perigos advindos de registros dessa categoria de dados que tem a ver com a esfera de convicção pessoal (religião, filosofia e opção sexual), com esfera de opção política e sindical e com a esfera de sua conformação pessoal (origem racial e ética dos dados genéticos de saúde).

Alguns países como é o caso de Portugal, incluíram entre os dados sensíveis os dados de vida privada, ampliando sobremaneira a categoria. Essa forma a proteção que se confere ao indivíduo vem tanto ampliada quanto cercado das dificuldades de sua delimitação. Havendo motivos de interesse público importantes sobre a reserva de serem prestados às garantias adequadas, admite-se que os Estados-Membros estabeleçam outras exceções a prevenção e tratamento de dados sensíveis além daquelas anunciadas na Diretiva 95/46, em seu art. 8.

Em alguns estados membros da Comunidade Europeia, a coleta e o tratamento de dados sensíveis pode ser precedida de autorização prévia da autoridade pública de controle dos dados pessoais.

4.3 O alcance dos princípios

A tutela dos dados pessoais tem amplo alcance, no plano objetivo, em relação aos meios ambientes e formas de tratamento, e nos objetivo, referente aos polos ativo e passivo das obrigações impostas e eventuais a terceiros.

Os princípios inerentes aos dados pessoais são aplicados a todas as formas de armazenamento (coleta), tratamento e reprodução (e transmissão), seja por meio manual, eletrônico, pela rede mundial de computadores, a qualquer conjunto organizado de dados pessoais, seja qual for forma ou modalidade de sua criação, armazenamento organização e acesso.

Para Elvira L. Diaz (2013, p.294), o ciclo de operação da informação de dados, protegidos pela privacidade, compreende: (a) compilação, em que há limites objetiva privacidade, referente ao consentimento para a inclusão dos dados, na base de dados, e outro objetivo, que diz a respeito à exclusão dos dados sensíveis, devendo ser observados os princípios da veracidade e adequação; (b) processamento, que incidem de forma especial aos princípios da segurança e

transparência; (c) resultados do tratamento, em que a síntese do cruzamento de dados dos distintos arquivos da base de dados e o alcance deles devem ser informados ao titular; (d) transmissão e difusão que é a etapa de maior potencial lesivo à privacidade/intimidade pessoal.

De La Cueva (2013, p. 58), acrescenta que os princípios e a tutela protetiva dos dados pessoais são aplicados também aos novos campos das telecomunicações, vídeovigilância, *internet*, bem como a novos perigos provenientes de etiquetas inteligentes, chips incorporados a pessoas, pulseiras eletrônicas; dados biométricos e etc.

No plano do alcance objetivo da tutela dos dados pessoais, grande parte das leis estrangeiras estabelece quatro ou cinco categorias de pessoas: o titular do dado, seu destinatário, o responsável pelo tratamento, o sub contratante do tratamento e o terceiro.

No que tange ao titular do pessoal que será objeto do tratamento, há discussão se apenas é a pessoa física ou se também alcança as pessoas jurídicas. Tal discussão tem origem na doutrina sobre quem pode ser sujeito à privacidade. Não há dúvida, porém, que o destinatário dos dados pessoais podem ser tanto pessoa física, como pessoa jurídica que recebe esses dados. O destinatário é quem recebe os dados pessoais; é o responsável pelo banco de dados ou cadastro; é a pessoa física ou jurídica, pública ou privada, que decide sobre a finalidade o conteúdo e o tratamento dos dados. O responsável ou encarregado pelo tratamento é a pessoa física ou jurídica, pública ou privada, que sozinha ou conjuntamente com outras pessoas tratam os dados. O subcontratante é a pessoa física ou jurídica, pública ou privada, que trata os dados pessoais por delegação do responsável pelo tratamento. O terceiro é a pessoa física ou jurídica, pública ou privada que não sendo titular dos dados, o responsável pelo tratamento, o subcontratante ou outra pessoa sob autoridade direta dessas duas últimas, esteja habilitada tratar os dados.

4.4 Direitos de defesa do titular dos Dados Pessoais

Direitos de defesa as primeiras medidas a disposição da vítima diz a respeito do direito de defesa para segurar os princípios inerentes dados pessoais.

4.4.1 Direito de acesso

O de acesso é a faculdade que possui o titular dos dados pessoais (DE LA CUEVA, 2013, p. 32 e 75) para solicitar e obter do responsável um cadastro de informações sobre os mesmos dados que estão em seus arquivos. É a primeira medida de defesa e que docorre diretamente no princípio do livre acesso aos dados pessoais pelo seu titular (art. 5º, inc LXXII, a, da Constituição Federal e art. 43, caput, CDC).

Ao titular da foto, imagem, texto, comentário, e-mail e etc, é assegurado o direito material de acesso às informações sobre o tratamento de dados pessoais que lhe digam respeito, desde a coleta até a transmissão. Tal direito é plenamente exercível pelo titular do lado pessoal do juiz competente. Em caso de falecimento ou sucessão provisória (ausência), esse direito pode ser exercido pelos sucessores, pelo inventariante do espólio ou pelo representante ou procurador ausente.

O direito é acesso, conforme o art.12, a, da Diretiva 95/46 da Comunidade Europeia(1995, p. 42), compreende: (a) a confirmação de terem ou não sido tratados das que lhe digam respeito informações sobre, pelo menos, os fins a que se destinam esse tratamento, as categorias de dados acessados e os destinatários a quem serão enviados os dados; (b) a comunicação inteligível dos dados que estão sujeitos a tratamento e as informações disponíveis sobre as origens dos dados; (c) o conhecimento da lógica inerente ao tratamento dos dados.

Em alguns países, o de acesso é subdividido por dois direitos distintos: o direito de acesso ao dado stricto sensu e o direito de informações, que compreende a ciência dos aspectos acima mencionados.

4.4.2 Direito à retificação

Em decorrência do princípio da veracidade, o titulado do dado tem o direito de retificá-lo ou torná-lo exato. O direito à retificação (DE LA CUEVA, 2013, p. 77), compreende a faculdade que esse titular tem para obter a correção ou complementação dos dados pessoais que se encontram inexatos ou incompletos em um banco de dados. A exatidão da informação compreende também a sua clareza e objetividade.

Nos termos do artigo 4º da Lei 9507/1997, art. 5º inc. III, da Lei 12414/2011 e o art. 43 inc. III do CDC e/ou art. 5 inc. II da Constituição Federal e o princípio da veracidade, o titular do dado pode exigir diretamente ou judicialmente do responsável pelo armazenamento, tratamento ou transmissão de seus subcontratos e terceiros que estão de posse dos dados pessoais, à retificação e qualquer informação equivocada em seus bancos de dados sejam de caráter público ou privado.

4.4.3 Direito de vinculação a finalidade

O direito de uso conforme o fim (ou de vinculação a finalidade) é a faculdade do titular de exigir que o dado pessoal seja destinado aos objetivos para quais foi fornecido.

Trata-se aqui, (VALDÉS, 2006, p.71), de uma modalidade defesa em que é possível restringir o tratamento, em qualquer de suas etapas, apenas a determinado fim específico, de uma obrigação de fazer, ou que pode também vetar certo uso do dado (obrigação de não fazer).

O dado ou informação pessoal constante em bancos de dados, entre os quais os ambientes de rede e da informação (como email, intranet e redes sociais), devem preservar os princípios da adequação e da finalidade, de modo que, a princípio, não podem ser utilizados para fins diversos daqueles que motivaram o seu armazenamento, sem o consentimento do seu titular. É justamente essa tutela que esse direito de defesa visa resguardar.

Pelo Direito de vinculação à finalidade, o titular do dado pessoal pode requerer, em juízo ou fora dele, a limitação do seu uso ou de sua circulação apenas para fins a que se destina.

4.4.4 O direito ao cancelamento

O direito ao cancelamento ou à eliminação tem como fim destruir informação pessoal sensível em razão da inobservância de princípios afetos aos dados pessoais. Conforme, De La Cueva (2013, p. 79), objetivo do direito ao cancelamento

é eliminar do cadastro tais dados, isso porque nunca deveriam ser registrados em tais bancos, ou porque, mesmo tenha sido recolhido legalmente, existe causas que exigem a sua supressão.

Pablo de La Cueva (2013, p. 69), destaca ainda que, mediante a uma causa justificada, o consentimento pode ser revogado, ainda que sem efeitos retroativos. O art. 5 da Lei 12.414/2011 prevê o direito do cancelamento do cadastro positivo pelo titular do dado. O CDC não tem norma no mesmo sentido, pois, à semelhança de outros bancos de dados, os dados contidos são usados em seu desfavor. Todavia é óbvio que, se o consumidor quitou o débito que o positivo é um cadastro de proteção de crédito, terá o direito de cancelamento do registro desabonador, pois a informação passou a ser inverídica.

Da mesma forma, no âmbito das novas tecnologias, da Internet e de suas aplicações, deve ser garantido ao titular da informação (mensagem, texto, vídeos, fotos e etc.) o direito de apagar a informação pessoal que lhe diga respeito e que não corresponde à realidade, ainda que se exija, em alguns casos motivação. Haverá o direito de cancelamento quando observados os princípios afetos aos direitos pessoais

4.4.5 Direito ao esquecimento

O direito ao esquecimento é a faculdade que o titular e o lado pessoal tem para vê-lo apagado, suprimido ou bloqueado, pelo decurso do tempo, por ter cessado sua finalidade ou por seus direitos fundamentais. Trata-se (ROJAS, 2013, p.2) de uma espécie de caducidade, em que a informação, pelo decurso do tempo, pela expiração de sua finalidade ou por sua proximidade com os direitos fundamentais afetos à personalidade, parece ou deveria perecer, ainda que por imposição da lei.

O tempo causa repercussão no Direito. ele é capaz de consolidar as situações pretéritas, ainda que lesivas ao Direito. A segurança jurídica e a paz social trouxeram ao Direito vários institutos, como prescrição, decadência, anistia, perdão, coisa julgada e etc. No bojo de cada um deles, há duas sementes comuns: o esquecimento do passado e a superação presente e futura.

Por isso, ao longo da História do Direito, foram surgindo e evoluindo diversos institutos que trazem em seu bojo a ideia do esquecimento, como elemento de conformação e pacificação social. O arrependimento, a maturidade e a evolução são intrínsecos ao humano, que, com seus erros, procuram corrigi-los e traçar novos rumos para o desenvolvimento.

Para Antônio Rulli Júnior e Antônio Rulli Neto (2012, p. 425), o direito ao esquecimento é um direito fundamental, associado a dignidade da pessoa humana e a inviabilidade pessoal (arts.1, III, e art. 5, X, da Constituição Federal). Negá-lo é admitir pena de caráter perpétuo. O enunciado n. 531 aprovado na VI Jornada de Direito Civil, consigna que “a tutela da dignidade da pessoa humana na sociedade da informação inclui o direito do esquecimento”. Trata-se, na verdade, de mera consequência lógica do direito está (só estágio de solidão), no qual a pessoa quer, na verdade que se esqueçam dela.

A quarta turma do STJ no resp. n. 1334.097/RJ25, reconheceu, por unanimidade, o direito ao esquecimento de pessoa que fora acusada e absorvida na participação de um grave crime ocorrido no Rio de Janeiro, confirmando a condenação por dano moral imposta a um veículo de comunicação social.

Também a Corte Europeia de Justiça²⁶ referiu-se ao direito ao esquecimento é fácil do resultado de buscas realizadas na Internet, o qual envolvia informação pessoal desatualizada de um cidadão espanhol.

Direito de esquecimento tem particular incidência em relação à história judicial, aos dados pessoais, à circulação de informações na Internet e às sombras do passado. Todos possuem de algum modo, uma relação com pelo menos uma forma de exposição à privacidade. Embora o efeito prático da ordem judicial de cancelamento de um dado e de apagá-lo em face do esquecimento seja idêntico, o direito ao esquecimento não se confunde com aquele. O cancelamento não depende do transcurso do tempo ou da caducidade da finalidade. No esquecimento, o dado pessoal foi colhido corretamente e devidamente tratado. Em prol da dignidade da

²⁵ BRASIL. Superior Tribunal de Justiça. Recurso Especial n. 1.334.097/RJ. 4ª Turma. Relator Ministro Luis Felipe Salomão. Publicado em DJe de 10.9.2013.

²⁶ Corte Europeia de Justiça. Processo n. C-131/12. Google Spain S.L. e Google INC Agencia Española de Protección de Datos e Mario Costeja. Maio de 2014. Relator M. Ilesic.

pessoa humana, dos direitos fundamentais ou da caducidade (decorrente de sua provisoriedade), este dado é esquecido para que o titulado dado possa prosseguir sua vida.

Algumas situações impedem o exercício do direito ao esquecimento, entre as quais: quando os dados estão relacionados com a história, referiram-se a tema de interesse histórico ou decorram de fatos vinculados ao exercício de uma atividade pública de uma figura pública. Aplica-se a que admite ações afetas à privacidade.

Configura a caducidade temporal, a proximidade com os direitos fundamentais ou expirada à finalidade por não haver causa impeditiva, tem outro lado da do pessoal segurado direito ao esquecimento.

4.4.6 Direito a não sujeição a decisões individuais automatizadas

Trata-se de um remédio contra tratamento de dados que tem como objetivo traçar um determinado perfil da pessoa. Segundo, DE LA CUEVA (2013, p. 82), é um antídoto contra ameaça decorrente nas conclusões que podem resultar da interrelações de dados isolados que, por si só, tal como foram obtidos, não levam a qualquer impressão do indivíduo, mas que, quando passam pelo tratamento automatizado, produzem a definição das características da personalidade de uma pessoa em particular.

Esse direito é uma proteção absolutamente lógica, que decorre naturalmente dos postulados de Direito Constitucional e Civil, também presentes na ordem jurídica brasileira.

O Artigo 13 da Lei n. 67/1998 de Portugal, prevê o direito de não sujeição a decisões individuais automatizadas, cuja Regra geral assim dispõe:

Artigo 13.º

Decisões individuais automatizadas

1 - Qualquer pessoa tem o direito de não ficar sujeita a uma decisão que produza efeitos na sua esfera jurídica ou que a afecte de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspectos da sua personalidade, designadamente a sua capacidade profissional, o seu crédito, a confiança de que é merecedora ou o seu comportamento.

2 - Sem prejuízo do cumprimento das restantes disposições da presente lei, uma pessoa pode ficar sujeita a uma decisão tomada nos termos do n.º 1,

desde que tal ocorra no âmbito da celebração ou da execução de um contrato, e sob condição de o seu pedido de celebração ou execução do contrato ter sido satisfeito, ou de existirem medidas adequadas que garantam a defesa dos seus interesses legítimos, designadamente o seu direito de representação e expressão.

Esse direito é uma proteção absolutamente lógica que decorre naturalmente dos postulados de Direito Constitucional e Civil, também presentes na ordem jurídica brasileira.

O direito de não sujeição a decisões individuais automatizadas ocorre quando houve desvio de finalidade no tratamento de dados pessoais; não foi observada a adequação dentro dado pessoal e seu tratamento; o consentimento, caso seja necessário, foi viciado; ou quebrou-se a boa-fé, a lealdade e a transparência. Diante disso, o tratamento desses dados gerou um resultado mais intrusivo à privacidade do que os dados originalmente fornecidos (por exemplo, um aspecto da personalidade que não constava dos dados antes do seu tratamento), com repercussões no princípio da igualdade (por apresentar um fator sujeito de diferenciação). Esse resultado danoso e geralmente discriminado foi o único fundamento de uma decisão que trouxe consequências negativas na esfera jurídica do seu titular ou lhe afetou significativamente. Em outras palavras, houve um ilícito no tratamento de dados (invasão de privacidade) e uma decisão com repercussões jurídicas danosas ao titular dos dados, tomadas com base em um fator de discriminação.

No campo do Direito Constitucional no Brasil, a decisão individual automatizada é inconstitucional, no § 2º do art. 216 da Carta Magna. Ela viola o direito à privacidade, porque não são observados seus postulados; fere a igualdade e a causa discriminação, pois se utiliza de um fator injustificado de discrimine.

Já no campo do Direito Civil brasileiro, o consentimento dado pelo titular, nos casos que é exigido, de um erro ou dolo (arts. 138 e 145 do Código Civil), pois o titular fornecer os dados por ignorar sua real finalidade ou em função do uso. Houve desvio de finalidade e da adequação e foi quebrada transparência, boa-fé e a lealdade. O que torna o ato ilícito, art. 187 do Código Civil. O direito de não sujeição adesão individual automatizada também se aplica ao direito brasileiro, nas suas mais diversas áreas.

5 A PRIVACIDADE: NOVOS CONTORNOS REFLETIDOS PELA SOCIEDADE DA INFORMAÇÃO

A privacidade é um conceito amplo em matéria de proteção da autonomia individual e da relação entre um indivíduo e a sociedade (incluindo governos, empresas e outros indivíduos). A definição de privacidade varia entre países e indivíduos com base em experiências passadas e entendimentos culturais. A origem do termo privacidade vem da língua inglesa da palavra *privacy*. Segundo Sandra Lia (2008), privacidade é tudo aquilo que o indivíduo quer ocultar do conhecimento público.

Celso Bastos conceitua privacidade como a:

faculdade que tem cada indivíduo de obstar a intromissão de estranhos em sua vida privada e familiar, assim como de impedir-lhes o acesso a informações sobre a privacidade de cada um, e também impedir que sejam divulgadas informações sobre esta área da manifestação existencial do ser humano. (BASTOS, 1989, p. 63)

Uma crescente preocupação em relação à tutela jurídica da privacidade é uma questão, o direito a privacidade parece cada vez mais distante da realidade. A ideia de privacidade não é recente, e pode ser identificada em outras épocas e sociedades.

De acordo com Constant (1989), os povos antigos, as atividades eram submetidas a uma intensa vigilância, não havia "independência privada". A vida privada era centrada na vida em família. Diante da importância crescente dos dados na sociedade contemporânea nada mais natural que haja, na mesma proporção, uma preocupação crescente em relação à proteção do seu titular.

Para Díaz (1996) os cidadãos da Roma antiga, a casa, o lar doméstico, desempenhava um papel muito importante e era considerado um lugar santo, sagrado. Durante a idade média, a intimidade era um privilégio para poucos, para os senhores feudais, que detinham a propriedade, inclusive de seus vassalos. Nessa época, a intimidade era uma prolongação da propriedade, ou melhor, a propriedade era uma condição para ter privacidade. O entendimento filosófico da privacidade como pressuposto fundamental do homem enquanto pessoa surgiu antes de sua concepção jurídica, a partir do pensamento cristão. Santo Agostinho descobre a

intimidade, o homem sozinho refletindo sobre si em sua relação com Deus. Em 1958, o Tribunal de Séné, na França, reconheceu à família o direito de não publicação da imagem de uma atriz famosa e seu funeral.

Porém, começou a se aproximar das características atuais somente no século XIX, e se apresentar como distinguimos nas ultima décadas, principalmente após o surgimento da Internet . Essa nova usualidade da privacidade foi marcada a partir do famoso artigo THE RIGHT TO PRIVACY, de Samuel D. Warren e Louis D. Brandeis em 1890, onde surgiu a primeira manifestação individual de “ser deixado só”. No artigo autores colocam em evidência a ocorrência de transformações sociais, políticas e econômicas, bem como o surgimento de novos inventos, como a fotografia, que contribuíram para a ocorrência de violações da vida privada das pessoas.

Conforme Zanini (2014) partindo desses problemas, os autores analisam um bom número de decisões de tribunais ingleses e americanos, deduzindo então a existência de um princípio geral na *common law*, o *right of privacy*. Ou seja, o direito a privacidade. Ele denunciava que fotógrafos e empresas jornalísticas invadiam o recinto sagrado da vida privada e doméstica. A vítima teria sido o próprio Samuel Warren, que era inconformado com a intromissão da imprensa em sua vida familiar. Um trecho do artigo:

1. O direito a privacidade não proíbe qualquer publicação da matéria que é de interesse público ou geral. [...] 2. O direito à privacidade não proíbe a divulgação de qualquer matéria, apesar de sua natureza privada, quando a publicação é feita mediante circunstancias que tornem uma informação privilegiada de acordo com a lei de calúnia e difamação. [...] 4. O direito à privacidade cessa após a publicação dos fatos pelo individuo ou com seu consentimento. [...] Os remédios para uma invasão do direito a privacidade também são sugeridos por aqueles administradores da lei de difamação e na lei da propriedade literária e artística, nomeadamente: 1. Uma ação de responsabilidade civil por dados em todos os casos. (WARREN E BRANDEIS, 1890)²⁷

²⁷ I. The right to privacy does not prohibit any publication of matter which is of public or general interest.[...] 2. The right to privacy does not prohibit the communication of any matter, though in its nature private, when the publication is made under circumstances which would render it a privileged communication according to the law of slander and libel.[...] 4. The right to privacy ceases upon the publication of the facts by the individual, or with his consent. The remedies for an invasion of the right of privacy are also suggested by those administered in the law of defamation, and in the law of literary and artistic property, namely :- I. An action of tort for damages in all cases.

Warren e Brandeis (1890) consideram em seu artigo que a invasão da privacidade, se configura como uma profunda ofensa, que lesionando a noção do indivíduo sobre sua individualidade, dignidade, independência e honra. O fato de que um artigo publicado em 1890 ainda continue a ser considerado hodiernamente como a obra fundamental sobre o tema, sem ter perdido sua validade, especialmente se levarmos em conta a importância e atualidade da matéria.

Interpretam Zagol e Tibiriçá (2011) que, em algumas culturas focam mais nos direitos da comunidade do que nos direitos individuais, outros, como países da Europa e Brasil que adotam o *civil law*, são sensíveis aos direitos de privacidade em razão dos abusos sofridos na Segunda Guerra Mundial. Tecnologias modernas de comunicação proporcionam uma importância muito maior a privacidade e o controle de informação.

Adeptos da livre circulação de dados se pronunciaram na Convenção Internacional das Telecomunicações em Torremolinos – Málaga, e por sua vez a Suécia, através da Lei denominada Datalagen (Lei n. 289), passou a exigir uma autorização especial para a transmissão de dados recolhidos na Suécia para o estrangeiro, dando o primeiro passo para se regulamentar o tratamento informatizado de dados pessoais, prevendo a proteção ao seu titular. Ainda conforme leciona Perez Luño (pag. 36, 1996), no mesmo ano de 1973 e depois 1974, o Comitê de Ministros do Conselho da Europa, através de duas Resoluções²⁸, a primeira referente à proteção da vida privada das pessoas físicas frente aos bancos de dados eletrônicos no setor privado e a segunda sobre os bancos de dados no setor público, recomendava aos países membros a adoção de medidas legislativas que garantissem determinados princípios²⁹.

²⁸ Tais textos foram os primeiros documentos internacionais a se referirem à proteção de dados pessoais.

²⁹ São exemplos destes princípios o direito dos interessados em conhecer e acessar as informações que lhes digam respeito; a obrigação dos bancos de dados públicos ou privados de corrigir a informação inexata e cancelar a obsoleta, irrelevante ou obtida por procedimentos ilegais; a adoção das garantias correspondentes para impedir que a difusão de dados estatísticos permita a identificação de sujeitos individuais e para evitar a transmissão de dados a pessoas ou entidades não autorizadas.

Em 1970 a primeira lei federal de proteção de dados da Alemanha³⁰ entrou em vigor, obrigando repartições públicas e empresas privadas a observância de regras materiais determinadas no tratamento de dados pessoais e instituiu um valioso sistema de direitos civis e mecanismos de controle. Assim como a Suécia e a Alemanha, França (1978), Noruega (1978), Dinamarca (1978), Áustria (1978), Luxemburgo (1978) e Islândia (1979), dentre outros, também elaboraram leis referentes à proteção de dados pessoais.

Porém, foi a elaboração, pelo Conselho da Europa, da Convenção para a proteção das pessoas com respeito ao tratamento automatizado de dados de caráter pessoal, firmado pelos Estados-Membros da então Comunidade Econômica Européia em 28.01.1981, que trouxe diretrizes claras a respeito da matéria.

A fim de tentar harmonizar a circulação de dados na Europa com a proteção dos dados pessoais foi elaborada, em 1995, a Diretiva 95/46/CE pela União Europeia, que na sua exposição de motivos³¹ faz constar duas antigas ambições do projeto de integração europeia, quais sejam, a realização de um mercado interno – auxiliado pela livre circulação de informações pessoais – e a proteção dos direitos e das liberdades fundamentais das pessoas. Em suas disposições finais a Diretiva estipulou um prazo de três anos, a contar da data de sua adoção – portanto vencendo em 1998-, para que os Estados-Membros dessem cumprimento à Diretiva, elaborando sua legislação nacional ³².

Finalmente, cumpre destacar que a questão da proteção dos dados pessoais ganhou a atenção da América Latina. Em 1999, o Chile inaugura a discussão entre os países latinos e publica sua lei de proteção de dados (Ley nº 19.628/99). Em 2000 foi a vez da Argentina (Ley 25.326/2000) e em seguida Uruguai (Ley nº

³⁰ Lei de Proteção de Dados do estado federal de Hesse, que entrou em vigor em 1970, é considerada a primeira lei formal de proteção de dados do mundo.

³¹ Conforme as considerações expostas no item 3 da Diretiva 95/46/CE, “o mercado interno europeu, que tem assegurada a livre circulação de mercadorias, pessoas, serviços e capitais, a teor do art. 7. do Tratado da União Européia, exige não só que os dados pessoais possam circular livremente de um Estado-membro para outro, mas também que sejam protegidos os direitos fundamentais das pessoas”.

³² Cabe mencionar ainda a Diretiva 97/66/CE, de 15 de dezembro, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das telecomunicações, que tratou de traduzir os princípios dispostos na Diretiva 95/46/CE em regras específicas para o setor das telecomunicações e a Diretiva 2002/58/CE da União Européia, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas, que revogou expressamente a Diretiva 97/66/CE.

18.331/2008), Paraguai (Ley nº 1.682/01) e México (Publicada no Diário Oficial em 05.07.2010) . A Colômbia teve seu projeto de lei aprovado em 16. 12.2010 pelo legislativo e agora caminha para sanção presidencial. Ainda o Peru também discute seu projeto de lei.

5.1 Tutela do direito a privacidade aos dados pessoais

O direito à privacidade aos dados pessoais encontra tutela em normas e internacionais, o que inclui a Declaração Universal dos Direitos Humanos, o Pacto Internacional de Direitos Civis e Políticos, a Convenção Europeia dos Direitos do Homem, a Convenção Americana de Direitos Humanos Organismos Internacionais, a Declaração Americana dos Direitos e Deveres do Homem, como também Tribunal Europeu dos Direitos do Homem e a Organização das Nações Unidas (ONU), Comissão de Direitos Humanos, que também tratam a respeito da proteção da privacidade aos dados pessoais.

5.1.1. Normais nacionais

O direito à privacidade tem um grau de importância muito grande na Constituição Brasileira. É um dos direitos de personalidade e, portanto, é revestido de característica própria de direito fundamental e cláusula pétrea. Em decorrência da amplitude do direito de privacidade, este pode ser atacado mais facilmente. a Constituição vigente no nosso país emprega duas expressões diferentes relacionadas à privacidade do indivíduo: a intimidade e a vida privada, o que, conseqüentemente, gera uma multiplicidade de entendimentos de uma doutrina que procura formular definições de cada uma delas e suas diferenças. A Constituição vigente no nosso país emprega duas expressões diferentes relacionadas à privacidade do indivíduo: a intimidade e a vida privada, o que, conseqüentemente, gera uma multiplicidade de entendimentos de uma doutrina que procura formular definições de cada uma delas e suas diferenças.

O art. 5.º, inciso X, da Constituição Federal tutela de forma autônoma o conceito de vida privada, distinguindo-o da intimidade. Presume-se, desta forma,

que o constituinte utilizou a expressão vida privada em sentido estrito, como uma das esferas da intimidade.

Uma das fontes da distinção constitucional entre intimidade e vida privada é a prática jurídica francesa, grande influenciadora da doutrina civilista ocidental, esta considera o direito de intimidade apenas como um aspecto mais restrito ao direito à vida privada. O art. 9º do Código Civil brasileiro emprega as expressões como sinônimas, a saber:

Toda pessoa tem direito ao respeito de sua vida privada. Os Juízes podem, sem prejuízo da reparação do dano sofrido, ordenar todas as medidas, tais como sequestro, embargo e outras, aptas a impedir ou fazer cessar um atentado à intimidade da vida privada; essas medidas podem, se houver urgência, ser ordenadas em liminar.

Apesar de a Constituição Brasileira diferenciar o direito à intimidade do direito da vida privada, os doutrinadores permanecem a entender que esses dois direitos devem ser tratados como sinônimos. A vida privada não é um conceito que permanece imutável no espaço e no tempo. Zagol e Tibiriçá (2011) comentam que este conceito unívoco pode variar conforme a sociedade e também depende da posição que cada indivíduo ocupa no momento específico, na sociedade específica. A vida exterior e a vida profissional são componentes da vida privada. A privacidade tem um caráter mais subjetivo que muitas vezes impede uma resposta clara, harmônica e rápida aos problemas, explica Doneda (2006). A proteção de dados pessoais tem, em seu campo de aplicação, um caráter mais objetivo, para proteger o dado em si e, através dele, a pessoa”, o autor conclui, lembrando que as regras de proteção de dados pessoais costumam ser muito mais concretas, específicas e impor obrigações.

A proteção à personalidade encontra sua garantia na cláusula geral da personalidade, que tem como valor intangível, a dignidade da pessoa humana, princípio consagrado constitucionalmente e integrador do ordenamento pátrio. Tal princípio norteia as relações públicas e privadas de forma a pôr fim na divisão taxonômica a qual usualmente se aplica às relações jurídicas e pretende distinguir e definir os direitos de personalidade de outros direitos. Quer seja sua natureza de um direito fundamental, quer seja de um direito de personalidade, a privacidade demonstra o ponto em comum para o qual o ordenamento caminha: à preservação

da dignidade humana. Leonardo Rosco e Bessa (2008), definem que esse encontro entre os direitos de personalidade e os direitos humanos.

5.1.2 Normas internacionais

Não existe, até o momento, um tratado global que trate especificamente da proteção. Contudo, como já exposto, a Declaração Universal dos Direito Humanos (1948), Pacto Internacional Sobre os Direitos Civis e Políticos (1966) e a Convenção Americana sobre Direitos Humanos (Pacto de São José, em 1969), que asseguram a não interferência da vida privada e familiar da pessoa, do seu lar e da sua correspondência.

A Declaração Universal dos Direito Humanos em seu art. 18º prevê que, “ninguém será sujeito a interferências na sua vida privada, na da sua família, no seu lar ou na sua correspondência”. Já o Pacto Internacional dos Direitos Civis e Políticos proíbe expressamente “ingerências arbitrária ou abusivas” na vida privada e familiar da pessoa humana, em seu art. 17.

Além disso, com relação aos dados sensíveis, essas normas internacionais vedam a discriminação em diversas formas (arts. 2º e 7º da Declaração Universal dos Direito Humanos, 1º, I, e art. 24º, do Pacto de São José, e art. 25º do Pacto Internacional dos Direitos Civis e Políticos).

5.2 Teorias da privacidade

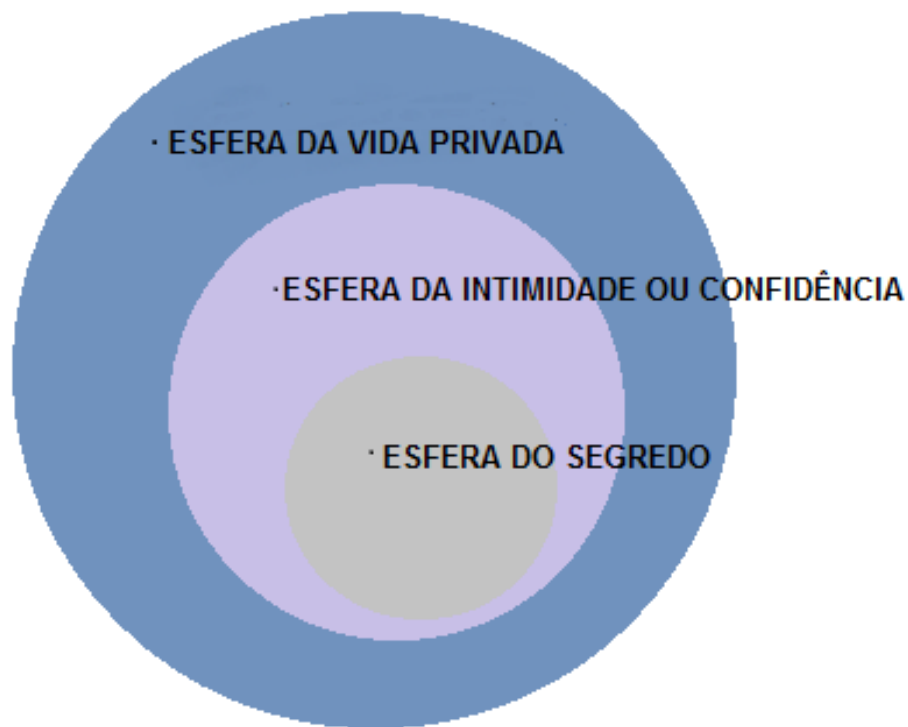
Duas teorias procuram identificar como se opera a privacidade: a teoria dos círculos concêntricos (ou das esferas) e a teoria do mosaico.

5.2.1 Teoria Dos Círculos Concêntricos (ou das esferas)

Em 1957, Heirinch Henkel apresentou durante o Fórum Jurídico Alemão a Teoria dos Círculos Concêntricos ou das Esferas, baseado no grau de sujeição da pessoa às ingerências externas. Observou-se, por meio desta, que a liberdade de informação e o direito à privacidade compõem círculos concêntricos de proteção e conhecimento. Hidemberberg ainda afirma que:

A esfera privada (o círculo da vida privada no sentido amplo) encerra três círculos concêntricos(camadas dentro de camadas): o círculo da vida em sentido restrito (a camada superficial), que contempla o círculo da intimidade(camada intermediária), no qual se acomoda o mais denso desses três compartimentos, o círculo do segredo(núcleo). (2006, p.80)

Figura 3: Teoria dos Círculos Concêntricos



Fonte: Produzido pela autora

O maior expoente e grande importador da teoria no Brasil foi Paulo José da Costa Jr.(2007, p.23) explicou este autor que subsistem diferenças entre a “‘esfera individual’ (proteção à honra) e a ‘esfera privada’ (proteção contra a indiscrição)”. Para ele, as condutas mais encobertas e secretas de uma pessoa correspondem à esfera privada, enquanto as mais abertas pertencem à esfera individual. São exemplos desta esfera o direito ao nome e à reputação.

A esfera privada é notadamente mais interessante aos estudos do autor. Conforme ele mesmo expõe:

Aqui, não se trata mais do cidadão no mundo, relacionado com os semelhantes, como na esfera individual. Trata-se, pelo contrário, do cidadão na intimidade ou no recato, em seu isolamento moral, convivendo com a própria individualidade. (COSTA JR., 2007, p. 24)

Considerando os estágios apresentados, a esfera da privacidade corresponde ao estágio do anonimato, da intimidade como o estado de intimidade, o segredo equivalente da reserva. A solidão, o último estágio da intimidade pessoal, seria um ponto dentro da espera do segredo.

5.2.2 Teoria do Mosaico

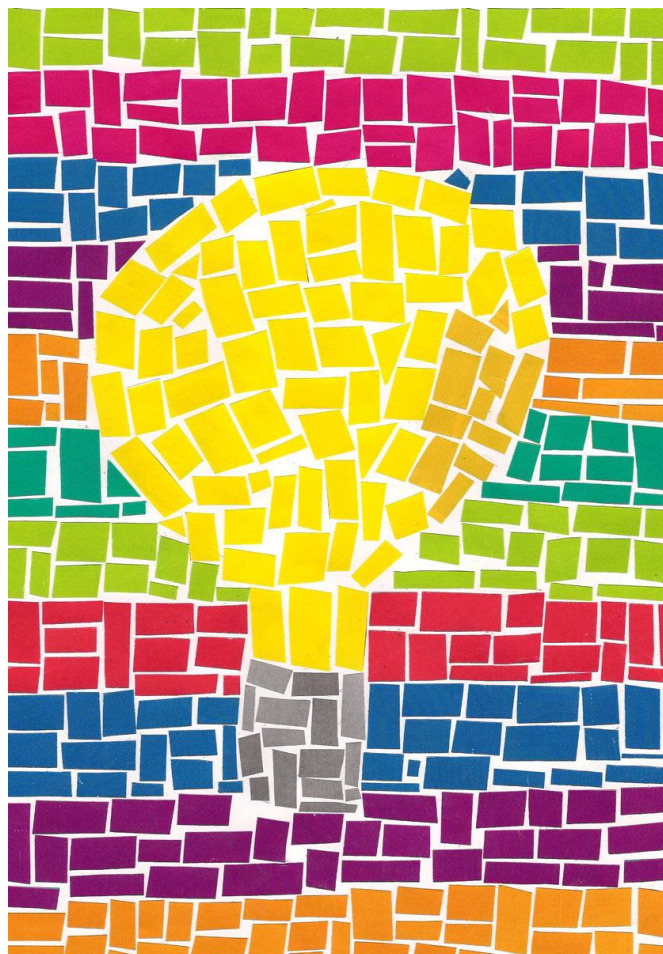
Diante da teoria das esferas, e sua insuficiência, para enfrentar novas e sofisticadas formas de ataque a privacidade através das novas tecnologias. Fulgencio Madrid Conesa, elaborou uma nova teoria, a Teoria do Mosaico:

existem a prioridades e relevantes do ponto de vista do direito à privacidade e que no entanto conectados com outros talvez e relevantes também podem servir para tornar totalmente transparente a personalidade de um cidadão como acontece com pequenas pedras que formam os mosaicos que se não dizem nada mas unidas formam um conjunto cheio de significados (CONESA, 1984, p.45, tradução nossa)³³

Conesa (1984), já havia contemplado, anos atrás, o perigo do tratamento informático dos dados ou informações pessoais que, se bem isoladamente considerados, não possuíam caráter íntimo, e sendo submetidas a esse procedimento, pudessem elaborar um perfil pessoal do indivíduo. Para fazer frente a esta situação propôs esse autor a teoria do mosaico. Onde ao reunir pequenas peças (dados) sem um significados, ao estruturar de forma que organizada, foram uma figura (informação) com total sentido, conforme a figura 4.

³³ existen datos a priori irrelevantes desde el punto de vista del derecho a la intimidad y que, sin embargo, en conexión con otros, quizá también irrelevantes, pueden servir para hacer totalmente transparente la personalidad de un ciudadano, al igual que ocurre con las pequeñas piedras que forman los mosaicos, que en sí no dicen nada, pero que unidas pueden formar conjuntos plenos de significados.

Figura 4: Exemplo de um mosaico



Fonte: Extraído na Internet.

Disponível em:<<https://teoriadacorblog.files.wordpress.com/2011/10/karineprg1a-mosaico.jpg>>³⁴

Não importa se a informação diz respeito à privacidade, à intimidade ou o segredo, mas sim o uso do que é feito dela. Os programas de informática usados para a criação e gestão de bancos de dados são capazes de criar um perfil do sujeito a partir da aplicação dos dados dispersos que só passam adquirir significado quando reunidos.

A teoria do mosaico é bastante útil para entender e explicar a invasão de privacidade pelo uso das novas tecnologias, contribuindo significativamente para a compreensão do problema da coleta e armazenamento de dados pessoais por entidades públicas e privadas. Ante esse panorama, cabe analisar se o direito à

³⁴ Acesso em: 03 de outubro de 2017.

intimidade foi capaz de evoluir e adaptar-se a esse novo desafio, que consiste na coexistência pacífica do uso cada vez mais constante das novas tecnologias e o respeito à intimidade das pessoas.

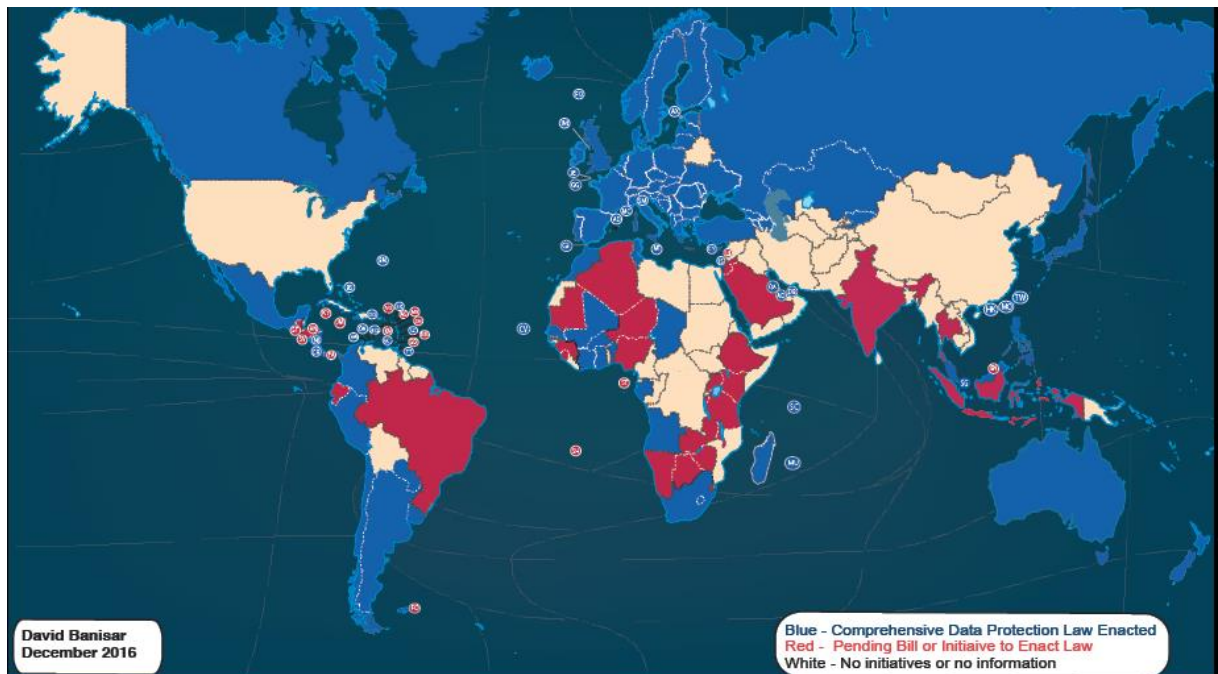
6. DADOS PESSOAIS SOB A ÓTICA DO ORDENAMENTO JURÍDICO BRASILEIRO

Neste capítulo será tratado os principais pontos sobre a Proteção de Dados Pessoais no Brasil, à legislação em que serve de amparo para essa proteção e sobre os projetos de lei que se encontram em elaboração.

6.1 A proteção de dados pessoais no Brasil

É instigante quando uma temática nova surge no Direito. Mesmo que o tema seja um novo já velho para alguns. Exatamente sob este prisma é que a proteção de dados pessoais deve ser analisada. No Brasil a discussão começa agora, com aproximadamente 40 anos de atraso em relação a países europeus e aos Estados Unidos, que têm legislação específica desde a década de 70. A seguir, Figura 5, para melhor visualização da situação do Brasil em relação ao mundo.

Figura 5: Situação do Brasil no mapa de Proteção de Dados Pessoais no mundo



Fonte: David Banisar - National Comprehensive Data Protection laws and bills³⁵.

³⁵ Banisar, DAVID. National Comprehensive Data Protection/Privacy Laws and Bills. 2016. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416> Acesso em: 03 de outubro de 2017.

O mapa é elaborado anualmente (sempre em dezembro) pelo pesquisador David Banisar, especialista em direito e políticas públicas e hoje conselheiro da ONG Artigo 19º, que trata de liberdade de expressão. Ele leva em conta quais países têm regras específicas em relação à privacidade e proteção de dados pessoais das pessoas, hoje, 110 países no mundo têm leis do tipo de regulação.

No final de 2010, através de uma iniciativa do Ministério da Justiça em parceria com o Observatório Brasileiro de Políticas Digitais do Centro de Tecnologia e Sociedade da FGV, foi proposto um debate com a sociedade através do blog Cultura Digital³⁶, sobre o anteprojeto de lei de proteção de dados pessoais a ser encaminhado ao legislativo no segundo semestre de 2011.

É uma pena que só agora o Brasil tenha se despertado para o grave problema acerca dos dados pessoais. Numa era em que a tecnologia permeia todos os setores, o titular dos dados encontra-se totalmente vulnerável, sem saber quais dados seus foram armazenados, disponibilizados, acessados sem consentimento, ou seja, tratados de alguma forma. Porém, esse é o momento da sociedade se mobilizar, de conhecer esse projeto de lei que será encaminhado ao legislativo, de questionar práticas abusivas em relação ao tratamento dos dados pessoais, enfim, de discutir o futuro das relações informatizadas, ou seja, do próprio ser humano.

A falta de uma lei específica para proteção de dados no Brasil nos trás uma total insegurança jurídica, “os direitos não nascem todos de uma vez. Nascem quando devem ou podem nascer” (BOOBIO, 1992, p.6). Com toda essa evolução, parece que é a hora de o Brasil possuir uma lei específica que trate de Dados Pessoais. É importante para o cidadão brasileiro, para o mercado e toda sociedade, estamos atrasado nesse processo. Estamos atrasados nesse processo, não há dúvidas da oportunidade e da necessidade estratégica da existência de uma regulação que trate sobre. No Brasil ainda não existe ainda uma lei geral sobre proteção de dados pessoais. É possível apenas fazer alguns recortes em dispositivos legais.

³⁶ Disponível em: <<http://culturadigital.br/dadospessoais>> Acesso em: 03 de outubro de 2017.

A Constituição Federal em seu art. 5º, inciso X, considera invioláveis a liberdade, a vida privada e a intimidade:

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

[...]

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

Ainda na nossa Carta Magna no seu art. 5º, inc. LXXII, quando é tratado o Habeas Data:

Art. 5, LXXII - conceder-se-á habeas data:

a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;

a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;

b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;

Na Lei nº 8.078 de 11 de Setembro de 1990, do Código do Consumidor, em seu art. 43º que dispõe sobre cadastros de proteção ao crédito:

Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

§ 1º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.

§ 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.

§ 3º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.

§ 4º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.

§ 5º Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.

Porém, o Código de Defesa do Consumidor não só protege os dados cadastrais, pois o Código como um todo protege o consumidor, resguarda também todos os dados relativos à relação de consumo, já que os dados pessoais são indistinguíveis a personalidade de qualquer cidadão. Então, se o consumidor tem seus dados violados ou utilizados de forma errônea, tem todo o direito de se resguardar dessa lei para sua proteção.

Temos também a Lei nº 12.527, de 18 de novembro de 2011, denominada como Lei de Acesso a Informação – LAI, que trás em seu conteúdo a transparência da informação, como não existe uma lei específica para proteção de dados pessoais ela terminou trazendo consigo um sucinto “estatuto” para Proteção de Dados em seu conteúdo, mas não chega a suprir as necessidades. A lei prevê que os dados armazenados em órgãos públicos são transparentes, ou seja, a qualquer momento o cidadão pode solicitar acesso a essas informações. Porém, o acesso a informações pessoais de terceiros, a não ser que esteja no rol de exceções, que o titular dê consentimento ou tenha sido produzida a mais de 100(cem) anos. Ela também proporciona a cada cidadão o acesso total de seus próprios dados em qualquer que seja o órgão publico, gerando uma maior celeridade as necessidades do solicitante.

Art. 10. Qualquer interessado poderá apresentar pedido de acesso a informações aos órgãos e entidades referidos no art. 1º desta Lei, por qualquer meio legítimo, devendo o pedido conter a identificação do requerente e a especificação da informação requerida.

§ 1º Para o acesso a informações de interesse público, a identificação do requerente não pode conter exigências que inviabilizem a solicitação.

§ 2º Os órgãos e entidades do poder público devem viabilizar alternativa de encaminhamento de pedidos de acesso por meio de seus sítios oficiais na Internet.

§ 3º São vedadas quaisquer exigências relativas aos motivos determinantes da solicitação de informações de interesse público.

Art. 11. O órgão ou entidade pública deverá autorizar ou conceder o acesso imediato à informação disponível.

§ 1º Não sendo possível conceder o acesso imediato, na forma disposta no caput, o órgão ou entidade que receber o pedido deverá, em prazo não superior a 20 (vinte) dias:

I - comunicar a data, local e modo para se realizar a consulta, efetuar a reprodução ou obter a certidão;

II - indicar as razões de fato ou de direito da recusa, total ou parcial, do acesso pretendido; ou

III - comunicar que não possui a informação, indicar, se for do seu conhecimento, o órgão ou a entidade que a detém, ou, ainda, remeter o requerimento a esse órgão ou entidade, cientificando o interessado da remessa de seu pedido de informação.

[...]

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

§ 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:

I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e

II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.

§ 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido.

§ 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias:

I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;

II - a realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;

III - ao cumprimento de ordem judicial;

IV - à defesa de direitos humanos; ou

V - à proteção do interesse público e geral preponderante.

§ 4º A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância.

§ 5º Regulamento disporá sobre os procedimentos para tratamento de informação pessoal.

Por fim, a Lei nº 12.965, de 23 de abril de 2014, o Marco Civil da Internet, lei que foi idealizada para regular os direitos e deveres para o usuário da Internet no Brasil. Embora o Marco Civil legisle especificamente a respeito da Internet, ele trouxe diversos itens referentes a proteção de dados, essa lei passou por diversas discussões até sua forma atual. Principalmente em 2013 que mídia tratou sobre o Caso Snowden³⁷, que revelou casos de espionagem nos EUA e gerou crise para o governo Obama e debate sobre privacidade online em todo o mundo.

Art. 3º A disciplina do uso da Internet no Brasil tem os seguintes princípios:

I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;

II - proteção da privacidade;

III - proteção dos dados pessoais, na forma da lei;

[...]

Art. 7º O acesso à Internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

³⁷ GREENWALD, 2014.

- II - inviolabilidade e sigilo do fluxo de suas comunicações pela Internet , salvo por ordem judicial, na forma da lei;
- III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

Continuando no art. 7º, da lei nº 12.965, os incisos VII e IX nos trás o Princípio do Consentimento:

- VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de Internet , salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
[...]
- IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

Por fim, o inciso X do art. 7º, dispõe sobre a exclusão definitiva dos dados na rede:

- X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de Internet , a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;

A lei possuiu uma seção dedicada a proteção de dados pessoais, com o seguinte título:

Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas

Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de Internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.

§ 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.

§ 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

§ 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.

Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por

provedores de conexão e de aplicações de Internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

§ 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.

§ 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que ofereça serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

§ 3º Os provedores de conexão e de aplicações de Internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.

§ 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:

I - advertência, com indicação de prazo para adoção de medidas corretivas;
II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;

III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou

IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.

Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o caput sua filial, sucursal, escritório ou estabelecimento situado no País.

6.2 Projetos de leis para proteção dos dados pessoais no Brasil

Atualmente existem dois Projetos de Lei, que são os 330/2013, de autoria do Senador Antônio Carlos Valadares e o nº 181 de 2014, com autoria do Senador Vital do Rego.

Explanaremos somente sobre o nº 330/2013, um ponto interessante desse projeto é a sua proposta em debater com os cidadãos sobre a temática de Proteção de Dados Pessoais, pois nada mais benéfico para a população do que construção conjunta de uma Lei com autoridades e especialistas. O debate do projeto de no site Pensando Direito³⁸, controlado pelo Ministério Público, onde vários outros temas importantes para a evolução do nosso país também são debatidos.

³⁸ Disponível em: <<http://pensando.mj.gov.br/>> Acesso em: 03 de outubro de 2017.

Figura 6: Print da tela inicial do site “Debate Sobre a Lei de Dados Pessoais no Brasil”



Fonte: Site Pensando Direito

Logo no topo o site do debate apresenta seus objetivos:

Toda pessoa tem direito à proteção de seus dados pessoais. Esta lei tem por objetivo garantir e proteger, no âmbito do tratamento de dados pessoais, a dignidade e os direitos fundamentais da pessoa, particularmente em relação à sua liberdade, igualdade e privacidade pessoal e familiar, nos termos do art. 5º, incisos X e XII da Constituição Federal.

Mesmo que projeto de lei nº 330 seja de 2011, foi amplamente discutido por especialistas da área no Brasil e pelo Ministério Público. Depois de muita análise e discussão, disso o MP resolveu em fevereiro de 2015 abrir para que toda população pudesse dar a sua contribuição.

O debate público sobre o anteprojeto de lei de proteção de dados pessoais ocorrerá por meio de comentários sobre a minuta do projeto de lei. A participação nas discussões é aberta, todos são bem-vindos. Para que ela

ocorra da maneira adequada é fundamental ler os Termos de Uso do site, que se aplicam a todo o processo de discussão.

A ideia do debate, por outro lado, não deve ser a de um “chat” nem tampouco de um fórum convencional. É imprescindível esclarecer que o processo não pode ser encarado como um plebiscito: mensagens repetidas com o mesmo conteúdo por diversos participantes ou por uma mesma pessoa, comentários com muitos “concordo” ou “discordo” e, até mesmo, temas com diversos comentários não significam necessariamente sua inclusão ou ausência no texto do Projeto de Lei que será encaminhado ao Congresso Nacional após a sistematização.

Nesse sentido, os participantes devem tentar qualificar ao máximo suas contribuições para que os tomadores de decisão possam aproveitar da melhor forma possível as discussões nesse espaço, já que esse é o objetivo do processo.

As discussões do debate são divididas em eixos. É fundamental que as contribuições sejam postadas nas respectivas seções apropriadas do site, fazendo referência ao tema pertinente àquela seção. Muitos dos assuntos do anteprojeto podem ter conexão entre si. Dessa forma, cada usuário pode decidir o eixo mais pertinente para o seu comentário ou eventualmente, para fins de clareza, dividir sua contribuição entre os artigos presentes em cada um dos eixos. É importante postar os comentários no artigo, inciso ou eixo temático correto. Comentários postados em locais inadequados podem não ser considerados.

Toda a participação deverá ter por base a boa-fé e ocorrer de forma educada, sendo vedada qualquer forma de abuso. A discussão poderá ser moderada, de acordo com os termos de uso, que serão aplicados sempre que necessário.

Contamos novamente com sua contribuição para fortalecer a democracia na Internet !

No debate a projeto é dividido em vários “eixos” que classificam os artigos:

Escopo e aplicação – arts. 1º ao 4º

Dados pessoais, dados anônimos e dados sensíveis – arts. 5º, 12 e 13

Princípios – art. 6º

Consentimento – arts. 7º ao 11

Término do tratamento – arts. 14 e 15

Direitos do titular – arts. 16 ao 21

Comunicação, interconexão e uso compartilhado de dados – arts. 22 ao 27

Transferência Internacional de dados – arts. 28 ao 33

Responsabilidade dos agentes – arts. 34 ao 41

Segurança e sigilo de dados pessoais – arts. 42 ao 47

Boas práticas – arts. 48 e 49

Como assegurar estes direitos, garantias e deveres? – art. 50

Disposições Transitórias – arts. 51 e 52

Uma das partes mais importantes do Projeto de Lei são os artigos arts. 5, 12 e 13, que categoriza e classifica dados pessoais, dados anônimos e dados sensíveis, mas também convida o cidadão a apresentar sua opinião sobre.

No site os dados são conceituados e classificados:

O que se entende por dado pessoal?

O texto proposto adota a ideia de que dado pessoal é uma informação que pode ser ligada a uma pessoa. Representa qualquer dado que possa ser associado a um indivíduo, fazendo com que a aplicação da norma se

concentre sobre o poder que o indivíduo tenha sobre o seu próprio dado. A definição de dado pessoal pode influenciar o equilíbrio de poder entre o cidadão e aquele que coleta e utiliza seus dados. Colabore nesta definição! De forma quase oposta à ideia de identificação, os **dados anônimos**, por sua vez, são dados que se referem a pessoas que não podem ser identificadas – como dados estatísticos, por exemplo. Um dado anônimo, ainda que seja referente a uma pessoa (ou grupos de pessoas), **não permite a identificação de seu titular**. Qual a importância da não-identificação? Quais seus limites? Participe!

Há ainda na proposta a necessidade de definição dos “**dados sensíveis**”, que são dados cujo tratamento pode ensejar a discriminação do seu titular – por se referirem, por exemplo, à opção sexual, convicções religiosas, filosóficas ou morais, ou opiniões políticas. Os dados sensíveis, pelo potencial discriminatório que apresentam, de acordo com a proposta em questão, deveriam ser protegidos de forma mais rígida. Aqui, devemos debater qual o grau de proteção desses dados e os limites para seu tratamento.

Parte de conceitos é muito importante, pois como até o momento só existem pesquisas sobre o tema, o projeto de lei, que tem como objetivo final transformar-se lei. Com isso esses conceitos serão consolidados para um melhor entendimento, se moldando a sociedade brasileira.

7. OS IMPACTOS NA GESTÃO DO DADOS PESSOAIS

O mundo inteiro passa por uma mudança de paradigma com relação à privacidade e proteção de dados pessoais. Essa mudança visa não só proteger o cidadão, mas também fomentar uma sociedade e um mercado movido a dados. Uma lei sobre proteção de dados permite que o cidadão tenha uma melhor gestão sobre como suas informações são utilizadas por organizações, empresas e pelo governo. Ela tem por objetivo estabelecer padrões mínimos a serem seguidos quando ocorrer o uso de um dado pessoal, como a limitação a uma finalidade específica, a criação de um ambiente seguro e controlado para seu uso e outros, sempre garantindo ao cidadão protagonismo nas decisões fundamentais a este respeito. O impacto maior de uma lei sobre proteção de dados pessoais é o equilíbrio das assimetrias de poder sobre a informação pessoal existente entre o titular dos dados pessoais e aqueles que os usam e compartilham.

7.1 Gestão de dados pessoais e direitos fundamentais: riscos e oportunidades

A informação, como fenômeno a ser regulado pelo Direito, não passou despercebido pelo Constituinte Brasileiro. A Constituição Federal de 1988 regula o fenômeno da informação, direta ou indiretamente, por meio de diversos positivos, ao garantir, entre outros a livre manifestação do pensamento, o direito de resposta, o sigilo da fonte, o acesso à informação, a inviolabilidade da intimidade e da vida privada, bem como o sigilo das comunicações de dados, telegráficas e telefônicas. A constituição reconheceu, assim, os efeitos da circulação e da não circulação da informação, sobre os indivíduos e a sociedade, e buscou regular esses efeitos por meio do estabelecimento de diversos direitos fundamentais.

Interessante é que na sociedade contemporânea, caracterizada exatamente pelo fluxo intenso de informação a partir de uma moderna estrutura de comunicação e informação, muito outros direitos fundamentais tendem a serem afetados ou influenciados pelo fenômeno da informação.

Por exemplo, (i) o direito à igualdade pode ser violado a partir de decisões discriminatórias tomadas com base de dados raciais ou de imigrantes, prática

conhecida como racial *profiling*³⁹; (ii) a liberdade do exercício de trabalho pode ser afetada quando um candidato de emprego tem sua contratação recusada por constar em cadastros de pessoas que ajuizaram ações trabalhistas, as chamadas “listas negras”⁴⁰, (iii) se o livre exercício do trabalho também poderia ser violado a partir de exigências de testes genéticos como requisito para contratação, (iv) a proibição de embarque em aeronave de passageiros registrados equivocadamente lista de terroristas poderiam construir uma limitação à liberdade de ir e vir⁴¹ (v) reuniões em espaços públicos podem ser afetadas se os seus participantes forem filmados e registrados sem justificativa.

Vê-se, dessa forma, que a sociedade atual, o processamento e utilização de dados afetam não apenas os direitos fundamentais que expressamente regula o fenômeno da informação. Na realidade, o sistema de direitos fundamentais como um todo pode ser influenciado, positiva ou negativamente, por esse fenômeno. Afinal, há diversos exemplos que demonstram como a infraestrutura de comunicação e informação se tornou hoje indispensável para o exercício dos direitos fundamentais: a Internet revolucionou a liberdade de expressão, a comunicação interpessoal e a comunicação social, assim como os sistemas informáticos, transformam o mundo do trabalho, da administração pública e privada e do mercado. Sem os quais se tornou impossível livre o exercício de qualquer trabalho, ofício ou profissão, a livre expressão da atividade intelectual, artística, científica e de comunicação.

A importância do constitucional do processamento e da utilização de informações dá-se, portanto, a partir de três elementos principais: (a) dependência dos indivíduos em relação à infraestrutura de comunicação e informação; (b) os riscos individuais que o processamento e utilização de informação podem causar; (c)

³⁹ A Comparative Analysis of Anti-Discrimination and Data Protection Legislations . Disponível em: <[http://relearn.be/2015/training-common-sense/sources/software/pattern-2.6-critical-fork/PATTERN%2B_points/references/Bart%20Custers,%20%20Toon%20Calders,%20%20Bart%20Schermer,%20%20Tal%20Zarsky%20\(eds.\)%20Discrimination%20and%20Privacy%20in%20the%20Information%20Society_%20Data%20Mining%20and%20Profiling%20in%20Large%20Databases%20%202013.pdf#page=74](http://relearn.be/2015/training-common-sense/sources/software/pattern-2.6-critical-fork/PATTERN%2B_points/references/Bart%20Custers,%20%20Toon%20Calders,%20%20Bart%20Schermer,%20%20Tal%20Zarsky%20(eds.)%20Discrimination%20and%20Privacy%20in%20the%20Information%20Society_%20Data%20Mining%20and%20Profiling%20in%20Large%20Databases%20%202013.pdf#page=74)> Acesso em: 03 de outubro de 2017.

⁴⁰ Existem inúmeras decisões do TST sobre a ilegalidade “listas negras”, como exemplo o julgado em 02/04/2008 – rel. Min. Maria de Assis Calsing, 4ª turma, DJ 18-4-2008.

⁴¹ “no fly list”, são listas mantidas pelo governo Americano, onde até crianças são impedidas de embarcar por listas erradas. Notícias sobre em: <<https://www.theguardian.com/us-news/2015/dec/09/no-fly-list-errors-gun-control-obama>> ; <<http://edition.cnn.com/2015/12/07/politics/no-fly-mistakes-cat-stevens-ted-kennedy-john-lewis/index.html>> Acesso em: 03 de outubro de 2017.

a insuficiência do processamento e utilização de informações no sistema de direitos fundamentais como um todo.

7.2 Âmbito de proteção

Após a fundamentação desse direito, impende delinear as suas características e dimensões.

Primeiramente destaca-se que o direito fundamental à proteção dos dados regula uma ordem de informação e comunicação e na sua essência multidimensional, na medida em que busca equilibrar os vários interesses de usos e dos direitos de proteção, de defesa e de participação do indivíduo nos processos comunicativos.

O objeto de proteção constitucional é o processamento e a utilização dos dados e informações pessoais em geral. Segundo Marion (2005, p. 271), a relevância jurídica resíduo menos nos dados em si, mas no processo de coleta, armazenamento e utilização na transferência, a partir do qual são extraídas informações pessoais a serem utilizadas em um determinado contexto para determinados fins. Assim, entra em ação a proteção constitucional se a informação for usada para uma finalidade que cause riscos, ou considerado ilícitos a priori (como é o caso dos bancos de dados criados a fins discriminatórios). Assim, somente uma análise do contexto do uso das informações (ou das hipóteses previstas para a sua utilização), do conteúdo da informação, da finalidade de sua utilização e dos riscos aos cidadãos podem determinar a legitimidade de ação de tratamento de dados e informações pessoais.

O bem jurídico protegido por esse direito é duplo. Ele visa proteger, por um lado, a integridade moral da pessoa, como componente essencial da dignidade humana, e, por outro as liberdades em sentido amplo (como a liberdade de comunicação, de trabalho, locomoção, de informação e entre outros). Concluímos que esse é o entendimento mais apropriado, por reconhecer que o processamento de dados pessoais influencia o sistema de direitos fundamentais na sua totalidade.

O âmbito de proteção do direito fundamental à proteção dos dados pessoais pode ser concebido em uma dupla dimensão, conforme PIEROTH e SCHLINK:

Ele consiste ao mesmo tempo: (i) a proteção do indivíduo contra riscos que ameaçam a sua personalidade em face da coleta processamento e utilização e circulação dos dados pessoais, e; (b) na atribuição ao indivíduo da garantia de controlar o fluxo de seus dados na sociedade. (2005, p. 17)

O direito fundamental à proteção de dados enseja tanto um direito subjetivo em defesa do indivíduo (dimensão subjetiva) como um dever de proteção estatal (dimensão objetiva). Na dimensão subjetiva, a atribuição de um direito subjetivo ao cidadão acaba por se delimitar uma esfera de liberdade individual que não pode sofrer intervenção do poder estatal ou privado. A dimensão objetiva representa a necessidade de concretização e delimitação desse direito por meio de ação estatal, a partir da qual surgem deveres de proteção do Estado para a garantia desse direito em relações privadas.

7.2.1 Dimensão subjetiva

Na sua dimensão subjetiva, o direito fundamental à proteção de dados pessoais, constitui-se como um direito subjetivo de defesa, que atribui ao indivíduo espaço e liberdade e privacidade, não sujeito a intervenções estatais. No caso de violação de direito subjetivo, enseja que a intervenção cesse, e, em caso de uma provável violação, ele possibilita a tomada de atitudes preventivas para não ocorrência da violação.

O controle dos seus dados pessoais pelo indivíduo compõe um aspecto essencial da dimensão subjetiva do direito à proteção de dados pessoais. PIEROTH e SCHLINK (2005, p.19), abordam que, o conceito geral é do que, a princípio, o titular dos dados deve ter o controle da coleta, processamento, utilização e circulação dos seus dados pessoais. Afinal, tendo em vista que os dados se referem a ele influenciam a sua esfera de direitos, somente o titular pode determinar a extensão de circulação de seus dados na sociedade.

A atribuição do controle sobre os dados pessoais não é absoluta. Esse controle encontra seus limites, especialmente, no interesse público e no direito de terceiros. Dois critérios podem ser utilizados para determinar os limites de

autodeterminação: a necessidade de um determinado processamento de dados pessoais para atender a um fim legítimo protegido pelo ordenamento jurídico ou para o cumprimento de direito de terceiro; e; a pertinência temática (ou a de conteúdo) entre o tratamento de dados pessoais e a finalidade atingida. O primeiro pode ser aplicado da seguinte forma: se processamento de dados for necessário para atender um direito de terceiro, e este superar o direito à privacidade do indivíduo no caso concreto, feito exercício de ponderação, é possível limitar esse controle. O critério da pertinência temática tem seu fundamento no conceito de que, em geral, os riscos e danos à privacidade individual decorrem da descontextualização das informações pessoais, pois ferem a expectativa do titular dos dados e dificultam sua autoproteção.

Por exemplo, é direito do empregador requisitar ao candidato de um emprego os dados pessoais necessários para comprovar sua habilidade e capacidade para o emprego. Entretanto, a prática de exigir certidões negativas de débito, emitidas pelo serviço de proteção de crédito pode ser considerada ilegítima, por duas razões: por um lado, este dado é irrelevante à comprovação de capacidade do candidato a emprego, e por outro, ele diz a respeito de um dado da relação de consumo que nada a ver tem com o contexto da relação trabalhista.

Em relação a bancos de dados da Bolsa Família⁴², a transferência de dados pessoais dos beneficiários para outro órgão do governo pode se mostrar necessária para o cumprimento de políticas públicas e atendimento das finalidades de programas sociais. Por outro lado, a transferência desses dados, que revelam informações sensíveis sobre a situação financeira dos beneficiários, para o setor privado mostra-se, além de necessário e descontextualizada, extremamente arriscada para os indivíduos, podendo acarretar discriminação e estigmatização aos titulares dos dados.

Assim, percebe-se que em regra é autodeterminação do titular sobre os dados pessoais, salvo direito de terceiros ou interesse público predominante previsto

⁴² É um programa de transferência direta de renda, direcionado às famílias em situação de pobreza e de extrema pobreza em todo o País, de modo que consigam superar a situação de vulnerabilidade e pobreza. Disponível em: <<http://www.caixa.gov.br/programas-sociais/bolsa-familia/Paginas/default.aspx>> Acesso em: 03 de outubro de 2017.

em legislação. Isso enseja a necessidade de autorização legal o consentimento do titular dos dados para que a coleta, o processamento, a utilização ou a circulação de dados pessoais seja considerada legítima.

Além disso, o direito subjetivo à proteção de dados pessoais implica que as restrições legais a esse direito não possam acarretar a sua eliminação, sob pena de ser considerada inconstitucional. Marion (2005, p. 280) ressalta, no entanto, que, embora diversas tentativas tenham sido feitas para a descrição do núcleo essencial desse direito, a questão ainda é muito controversa.

De toda forma, seria possível formular a partir do princípio da dignidade humana e da inviolabilidade da intimidade também no direito brasileiro um núcleo fundamental desse direito, a luz do conceito de que nenhum indivíduo deve ser submetido a uma coleta processamento e circulações de dados pessoais ilimitadas.

7.2.2 Dimensão objetiva

Ao mesmo tempo em que o direito fundamental à proteção de dados atribui ao indivíduo um espaço de liberdade, ele retira do Estado objetiva a mente a possibilidade de intervenção, independente se o indivíduo exerce ou não o seu direito. Com essa mudança de perspectiva percebe-se que os direitos fundamentais possui também um conteúdo objetivo, para além do seu significado de direito de defesa subjetiva.

Ademais, Mendes (2012, p. 469), conclui, que quando a constituição confere a proteção dos direitos fundamentais, ela o faz não apenas como proteção do indivíduo, mas também por considerar de determinados valores merecem ser objetiva a mente protegidos, por serem condições e pressupostos da sociedade democrática.

A dimensão objetiva dos direitos fundamentais revela a necessidade de concretização desses direitos do legislador, que deve estabelecer as condições dos procedimentos de exercício do direito, bem como mecanismos de proteção do bem jurídico nas relações privadas. Da dimensão objetiva extraem-se, assim, direitos à organização e ao procedimento, e, direitos à proteção. Ambos pressupõe a ação

positiva do Estado, sem a qual o direito perderia a sua eficácia. Já no direito fundamental à proteção de dados, se sobressai esses dois tipos de ação.

8 ANALISES DOS CASOS CONCRETOS

O estudo sobre a proteção de dados pessoais tem pautado diversas publicações nacionais e internacionais, de artigos científicos até capas famosas revistas. Os estudos de casos concretos só provam que dessa proteção se torna cada vez mais necessária para nosso cotidiano. O uso indevido de dados pessoais já é recorrente no Brasil. Foram selecionados diversos casos, desde vazamento de informações de um banco de dados pessoais, à discussão sobre o uso de criptografia em aplicativos de mensagens instantâneas, passando por ações de vigilância estatal e as configurações das Smart TVs que atualmente são comercializadas.

8.1 Caso da SmarTV no Brasil

As Smart TVs vendidas no Brasil⁴³ captam o áudio das conversas ao seu redor. As fabricantes alertam seus clientes por meio da política de privacidade e dos termos de uso que acompanham o produto a não conversarem perto do aparelho sobre temas confidenciais ou íntimos, já que o aparelho, além de gravar os sons à sua volta, também pode enviá-los a terceiros, como empresas terceirizadas que são responsáveis pela ferramenta de áudio do dispositivo. Isso muda o modo de interação tradicional dos telespectadores. De certo modo, agora o televisor também assiste ao telespectador.

Em 2013, um blogueiro do Reino Unido realizou testes na sua Smart TV LG e constatou que a televisão estava enviando dados para os servidores da LG, inclusive arquivos de um pen drive que ele conectou ao dispositivo. Um detalhe interessante é que mesmo quando a opção para a transferência de dados havia sido desligada, a Smart TV continuou a transmitir os dados para os servidores da companhia. Ao questionar a fabricante sobre os fatos, o blogueiro recebeu uma simples resposta de que ele havia assinado os termos de uso e serviço quando

⁴³ Fontes da notícia: <<http://doctorbeet.blogspot.com.br/2013/11/lg-smart-tvs-logging-usb-file-names-and.html>; <http://noticias.r7.com/recor-d-news/jornal-da-record-news/videos/rosana-hermann-comenta-caso-de-invasao-de-privacidade-atraves-de-smart-tv-17102015>; <http://exame.abril.com.br/tecnologia/noticias/samsung-pede-que-clientes-evitem-discutir-assuntos-pessoais-em-frente-de-sua-smarttv>> Acesso em: 03 de outubro de 2017.

comprou o televisor e que esse tipo de reclamação deveria ser feita ao vendedor do aparelho.

8.1.1 Analise do caso

A constatação de que as Smart TVs repassam a terceiros as informações por ela coletadas, mesmo os dados pessoais de um pendrive conectado a ela, vai contra o princípio da necessidade. O tratamento deve se limitar ao mínimo necessário para a realização das suas finalidades, abrangendo dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados. O conteúdo do pendrive do usuário claramente não é necessário para a funcionalidade da Smart TV. Mas não somente essa ação pode ser considerada desproporcional. O simples fato da coleta de áudio já viola os princípios da finalidade e da adequação. O primeiro prevê que “o tratamento deve ser realizado para finalidades legítimas, específicas, explícitas e informadas ao titular, não podendo ser tratados posteriormente de forma incompatível com essas finalidades”. O segundo presume que “o tratamento deve ser compatível com as suas finalidades e com as legítimas expectativas do titular, de acordo com o contexto do tratamento”, ou seja, a compra de um televisor, ao menos em princípio, não deve implicar na cessão dessa quantidade de dados pessoais, tendo em vista que o televisor consegue realizar suas funções normalmente sem gravar tudo o que acontece ao seu redor, o que ultrapassaria sua finalidade. Por sua vez, muitos consumidores não esperam que, ao comprar um aparelho de TV, sejam monitorados de forma ostensiva como demonstrado, o que viola a questão das legítimas expectativas do titular, sob o princípio da adequação.

8.2 O rastreamento de namorado

Em 2013, um app chamado “Rastreador de Namorado”⁴⁴ chamou a atenção por permitir monitorar as principais atividades de outra pessoa pelo celular, a partir das mensagens enviadas e recebidas, o registro de chamadas, e se o aparelho esteve desligado ou em modo avião. Para tanto, o app tem de ser instalado no

⁴⁴ Fonte da notícia: <<http://g1.globo.com/tecnologia/tem-um-aplicativo/noticia/2013/08/semconsentimento-app-rastreador-de-namorado-e-ilegal-diz-advogado.html>> Link do app:< <http://rastreador.denamorado.com.br/app>> Acesso em: 03 de outubro de 2017.

aparelho do “namorado” e configurado para notificar o celular da “namorada”. Todas as atividades relacionadas acima eram notificadas diretamente à namorada por meio de mensagens SMS.

8.2.1 Análise do caso

O consentimento do titular dos dados deverá ser livre, informado e inequívoco e fornecido por escrito ou por qualquer outro meio que o certifique. O app permite que qualquer pessoa com acesso ao celular de terceiros faça o download e torne o aparelho rastreável, ou seja, mesmo que o aplicativo requeira em seus termos de uso o consentimento de ambas as partes para seu funcionamento, é um risco claro que um dos namorados instale o aplicativo sem que o outro saiba. Para evitar tal desídia, a implementação do consentimento granulado, aquele que estende no tempo, periodicamente informando o titular do tratamento dos seus dados, pode ser uma saída.

8.3 O Site tudo sobre todos

Em 2015, surgiu na rede um site de nome Tudo sobre Todos45, no qual era possível consultar dados pessoais a partir de seu nome ou CPF. O modo de obtenção dessas informações é obscuro e provavelmente ilegal. A publicação desses dados na Internet de forma desprotegida e sem consentimento dos titulares se trata de um ataque frontal contra a privacidade dos cidadãos brasileiros.

A analista de planejamento Aline Oracic teve seus dados vazados e conta que ficou “bem assustada” ao ver expostas informações sobre ela, seus vizinhos e pessoas com quem mora. “Veja bem, se a pessoa precisa usar uma ferramenta como essa é porque eu não quero que ela tenha essas informações. Uma ferramenta dessas não foi desenvolvida para fins legais e não traz benefícios nenhum à população. Perigosíssimo esse site”, diz.

⁴⁵ Fonte da notícia: <<http://renatoleitemonteiro.jusbrasil.com.br/artigos/217037831/protecaao--de-dados-10-motivos-porque-o-site-tudo-sobre--todos-e-ilicito>> Acesso em: 03 de outubro de 2017.

8.3.1 Análise do caso

O funcionamento do site Tudo sobre Todos viola uma série de princípios de proteção a dados pessoais, tais quais a proteção à privacidade, a inviolabilidade da intimidade, da vida privada, da honra e da imagem, a finalidade, a adequação, a necessidade, o consentimento e basicamente todos os outros princípios da lei.

8.4 Criptografia e legalidade

Ministério Público Federal está realizando uma investigação sobre a legalidade da criptografia utilizada pelo WhatsApp⁴⁶, já que ela estaria em violação do inciso XII do artigo 5º da CF, que afirma que o sigilo da correspondência dos cidadãos brasileiros é inviolável, exceto quando se tratar de uma ordem judicial. Ou seja, a criptografia do WhatsApp estaria atentando contra o direito da Justiça de investigação com base na quebra de sigilo das correspondências.

A intenção do órgão investigativo é barrar o uso da criptografia, para que a Justiça tenha acesso facilitado às conversas no aplicativo quando estiver investigando casos criminais.

8.4.1 Análise do caso

A criptografia é reconhecidamente a melhor maneira para manter a segurança das comunicações no contexto digital para a proteção dos dados pessoais. A possibilidade de encriptação, classificando-a como uma possível medida de segurança utilizada para a proteção de dados em casos de incidentes de segurança, o que contraria a posição adotada pelo Ministério Público Federal. A proposta do MPF de tornar a criptografia ilegal parece desproporcional sob a ótica deste projeto, pois mais enfraquece a privacidade e segurança de dados pessoais durante o período de tratamento do que resolve o problema de investigação criminal de casos específicos.

⁴⁶ Fonte da notícia: <<http://www.tecmundo.com.br/whatsapp/104522-mpf-investida-possivel-in-constitucionalidade-criptografia-whatsapp.htm>> Acesso em: 03 de outubro de 2017.

8.5 Oi e vazamento de dados

Em 2013, a operadora Oi⁴⁷ foi acusada de entregar dados cadastrais de seus clientes aos provedores de conteúdo UOL e Terra. O MPF do Mato Grosso do Sul foi quem entrou com ação para investigar essa transferência de dados pessoais. A suspeita se iniciou após diversas denúncias de que os provedores citados acima começavam a ligar para oferecer seus serviços logo após a contratação da Oi. Mais do que isso, segundo a reportagem: “nas ligações feitas pelos representantes das empresas, os atendentes se passavam por funcionários da Oi e coletavam dados bancários e número do cartão de crédito dos clientes. Os consumidores eram, então, compelidos a contratar o serviço privado, para que, enfim, tivessem liberados *login* e senha de acesso à *Internet* .”

8.5.1 Análise do caso

A transferência a terceiros deve estar especificada e precisa contar com o consentimento do titular dos dados. Esse tipo de ação necessita do consentimento específico e próprio para ser realizado, o que já tornaria proibida as ações da Oi. Além disso, os responsáveis por causarem danos aos titulares devem responder solidariamente às acusações. Os órgãos competentes devem fiscalizar a comunicação e a interconexão de dados pessoais e entre outros aspectos. Sendo assim, podendo determinar, mediante processo administrativo, que sejam assegurados o contraditório e a ampla defesa, o cancelamento dos dados, o fim da interconexão ou outras medidas que garantam os direitos dos titulares. A Oi neste caso, de acordo com o que o órgão competente viesse a decidir sobre as acusações. No caso mais grave, a empresa poderia até mesmo ficar proibida de realizar tratamento de dados.

⁴⁷ Fontes da notícia: <<http://www.viomundo.com.br/denuncias/mpf-diz-que-oi-vazava-dados-sigilosos-de-clientes-para-uol-e-terra.html>>; <<http://www.otempo.com.br/cidades/procon-apura-fraudes-e-repasse-ilegal-de-cadastro-envolvido-oi-uol-e-terra-1.711715>> Acesso em: 03 de outubro de 2017.

8.6 Falha no APP do Banco do Brasil

Em dezembro de 2013, clientes do Banco do Brasil⁴⁸ que utilizam o aplicativo da instituição para gerenciarem suas contas bancárias vivenciaram, por um período de quase uma hora, uma falha que permitia a visualização de dados de outros clientes do banco. O BB afirmou que o problema foi prontamente corrigido, mas isso nos mostra que, mesmo os sistemas financeiros, que costumam ter protocolos de segurança elevados, podem possuir brechas graves que permitem episódios como esse para usuários comuns, que nem mesmo tentaram invadir ou quebrar a segurança do banco. Novamente, em 2016, a segurança dos sistemas de acesso online do BB, Caixa Econômica e Itaú mostraram novamente serem falhas. Um plugin “de segurança” utilizado pelos portais de acesso desses bancos revelou ter uma brecha que permite a criminosos acessarem os dados dos clientes. Segundo reportagem, “chamado de Warsaw, o plugin defeituoso em questão é utilizado por empresas como Caixa Econômica Federal, Banco do Brasil e Itaú.” A falha permite que criminosos utilizem a tecnologia para instalar um malware que enganaria o internauta fazendo ceder seus dados para hackers.

8.6.1 Análise do caso

O responsável pelo tratamento dos dados deve adotar medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Além disso, o responsável deverá comunicar ao órgão competente a ocorrência de qualquer incidente de segurança que possa acarretar risco ou prejuízo relevante aos titulares. Em episódios como esses, o banco teria que prestar contas ao órgão competente, que seria o responsável pela apuração e resolução do problema e por apontar possíveis prevenções a serem adotadas para casos futuros.

⁴⁸ Fontes da notícia: <<http://www.ebc.com.br/noticias/economia/2013/12/banco-do-brasil-suspende-aplicativo-que-provocoou-vazamento-de-dados>>; <http://olhardigital.uol.com.br/fique_seguro/noticia/plugin-de-seguranca-dos-bancos-permite-vazamento-de-dados-dos-internautas/58113>; <<http://meiobit.com/273531/falha-em-apps-expoe-dados-dos-clientes-do-banco-do-brasil>> Acesso em: 03 de outubro de 2017.

8.7 Colégio Bandeirantes e vazamento de dados de alunos

Em 2015, o tradicional Colégio Bandeirantes⁴⁹, de São Paulo, sofreu um vazamento de dados. Eles foram expostos em redes sociais e tinham registros de alunos, desde sua performance acadêmica até avaliações emocionais, feitas por professores e pela direção. A publicização desse conteúdo gerou mal-estar em toda a comunidade da escola, que rapidamente teceu críticas duras à direção por não ter um sistema de segurança eficiente para o armazenamento dessas informações.

Muitos alunos e pais se sentiram lesados com alguns comentários feitos nas avaliações vazadas. Uma delas diz, por exemplo: “tem olheiras, boca de ódio, cara de criança de filme de suspense”. O Bandeirantes sofreu fortes críticas e teve de mudar seu sistema de armazenamento. Esse episódio revela como a segurança da informação é importante em todos os âmbitos.

8.7.1 Análise do caso

O tratamento de dados pessoais de crianças só poderá ser realizado mediante o consentimento de seus pais, responsáveis legais ou por imposição legal.

Ademais, por se tratar de um caso que envolve adolescentes como titulares, que o tratamento deve ser especial, com maior ênfase na proteção, segurança e sigilo. O tratamento de dados pessoais de crianças e de adolescentes deve se dar no seu melhor interesse, de acordo com a legislação pertinente, a ver o Estatuto da Criança e do Adolescente. O princípio do melhor interesse nega a concepção clássica de que o menor de idade deva ser completamente tutelado por seus responsáveis e tenta dar voz ao interesse do menor na questão, ou seja, a vontade do jovem passa também a ser levada em consideração. É importante dar tratamento especial para o tratamento de dados pessoais de menores de idade, no entanto, o tratamento dado não leva em consideração a vontade do titular.

⁴⁹ Fonte da notícia: <<http://www.trrsecuritas.com.br/blog/2015/03/19/vazamento-de-dados-do-colegio-bandeirantes-causa-polemica/>> Acesso em: 03 de outubro de 2017.

8.8 Acesso não autorizado de funcionários

Outra situação que o acesso a grandes bases de dados possibilita é o assédio por parte de funcionários de empresas que oferecem, entre outros, serviços como Internet, telefonia e TV a cabo a clientes ou a possíveis clientes. Em 2015, várias pessoas, em especial mulheres, relataram casos nos quais atendentes entraram em contato com elas⁵⁰ após ter oferecido um pacote de serviços, utilizando o número da base de dados da empresa. Alguns, mesmo depois pedidos para encerrar a conversa, insistiam em continuar. Esse acesso a um grande número de telefones e e-mails a pessoas sem a devida responsabilidade e competência pode gerar inúmeros casos de abusos, assédios ou até mesmo perseguição. Por isso, é necessária uma política criteriosa sobre o acesso a bases de dados cadastrais dentro das empresas.

8.8.1 Análise do caso

Nesse caso, existem três figuras distintas que fazem parte da operação do tratamento: (a) O responsável (a pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais); (b) Operador (a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do responsável); (c) E o encarregado (pessoa natural, indicada pelo responsável, que atua como canal de comunicação perante os titulares e o órgão competente).

A figura do encarregado é parte da resposta a casos como esse, pois atua como ponte entre o titular e o órgão que realiza o tratamento dos dados e seus operadores. O encarregado, em casos como esse, deve ser ágil em responder a essas práticas de violação e vazamento de dados, indicar responsáveis e auxiliar os titulares. O tratamento dos dados pessoais, deve adotar medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados; o sigilo sobre os dados é obrigatório a todo agente de tratamento ou pessoa que teve acesso aos dados; torna-se dever do responsável a comunicação ao órgão competente de qualquer incidente de segurança que acarrete risco ou

⁵⁰ Fontes da notícia: <<http://taedai.com.br/quan-do-o-perigo-bate-a-porta>; <http://www.administradores.com.br/noticias/negocios/consumidores-denunciam-assedio-de-atendentes-de-telemarketing/101538/>> Acesso em: 03 de outubro de 2017.

prejuízo aos titulares; é responsável por averiguar o ocorrido e determinar ao responsável a adoção de providências, sendo possível até uma determinação de adoção de medidas técnicas que evitem que terceiros voltem a acessar os dados pessoais de titulares.

8.9 Privacidade do “POKÉMON GO”

“Pokémon Go” tornou-se um dos jogos mais populares no Brasil na metade de 2016⁵¹. Seu lançamento foi o mais aguardado do ano e sua jogabilidade transformou a experiência do uso de aparelhos móveis para muitos usuários. O jogo de realidade aumentada permite aos jogadores andarem pelas ruas e calçadas de suas cidades “caçando” pokémons. O mapa do jogo é o mapa da cidade. Logo, começaram as questões sobre a possibilidade do jogo estar espionando ou monitorando seus jogadores, os lugares aonde vão e, ainda, as imagens que cedem enquanto estão jogando, já que é necessário estar sempre com a câmera do aparelho celular ligada para jogar. Houve uma polêmica logo no lançamento do “Pokémon Go”, pois ele solicitava informações e permissões excessivas do usuário e de seu aparelho, como saber a página da web que o usuário acessou antes de abrir o app, assim como ler e escrever e-mails por você.

A Niantic, empresa desenvolvedora do game, logo diminuiu o nível de acesso do “Pokémon Go” aos dados e aplicações após a má repercussão, tornando os termos da política de privacidade do jogo mais aceitáveis e equiparáveis a outras aplicações de jogos. Contudo, nem todas as questões são abordadas nessa política e duas delas nos interessam neste estudo. A primeira se refere ao item 5 da política de privacidade do “Pokémon Go”, em que está expresso que, após o término ou desativação da conta ou contrato, a Niantic, seus clientes, afiliados ou provedores de serviço podem reter informações e conteúdo de usuário por um período comercialmente razoável para fins de fazer uma cópia de segurança, arquivamento ou auditoria. Já a segunda se relaciona à transferência internacional dos dados feita

⁵¹ Fontes da notícia: < <https://oglobo.globo.com/sociedade/tecnologia/produtores-de-pokemon-go-sao-processados-por-invasao-de-propriedade-19842815>>; <<http://www1.folha.uol.com.br/mercado/2016/07/1791219-pokemon-go-gera-duvidas-sobre-a-privacidade-dos-jogadores.shtml>>; <<http://www.otempo.com.br/interessa/pokemon-go-exp%C3%B5e-invas%C3%A3o-de-privacidade-por-aplicativos-1.1352100>> Acesso em: 03 de outubro de 2017.

pelo aplicativo e na qual fica autorizada a transferência de dados para países que possuem uma política de proteção de dados inferior a do país de origem.

8.9.1 Análise do caso

Duas questões levantadas na política de privacidade destacada. A primeira, diz que é direito do titular requerer a eliminação, a qualquer momento, de dados pessoais que tenham sido cedidos por ele. Ou seja, a política de privacidade do “Pokémon” estaria em desacordo com a legislação em uso no nosso país. O segundo ponto, referente à transferência internacional de dados, só é permitida para países que proporcionem nível de proteção de dados pessoais ao menos equiparável. Um terceiro ponto interessante que faz parte do debate diz respeito ao princípio da necessidade, pois não fica claro o porquê da política de privacidade do “Pokémon Go” requerer tantos dados e por tanto tempo. O tratamento aos dados devem sempre ser pertinentes, proporcionais e não excessivos.

8.10 Whatsapp integrado ao Facebook

Em 25 de agosto de 2016, o aplicativo de mensagens instantâneas WhatsApp anunciou que mudaria sua política de privacidade, compartilhando sua base de dados com a plataforma do Facebook⁵², empresa que comprou o aplicativo em 2014. Dessa maneira, os usuários foram instados a escolher entre aceitar ou não o compartilhamento de seus dados, tendo como prazo limite para optar pelo não compartilhamento o dia 25 de setembro de 2016. Aqueles que não responderam até essa data tiveram seus dados compartilhados. A transferência de dados é um assunto que os três projetos de lei deste estudo abordam de formas diferentes.

8.10.1 Análise do caso

A transferência de dados a terceiros com o consentimento do titular. No entanto, após o término da relação de tratamento de dados, a conservação das informações poderá ocorrer caso a finalidade seja transferência a terceiros. Ou seja,

⁵² Fontes da notícia: < <http://www.techtudo.com.br/noticias/noticia/2016/01/whatsapp-e-facebook-vao-compartilhar-dados-de-usuarios-indica-beta.html>>; <<http://g1.globo.com/tecnologia/noticia/2016/08/por-que-o-whatsapp-esta-dando-o-seu-telefone-para-o-facebook.html>> Acesso em: 03 de outubro de 2017.

caso um usuário do WhatsApp deixe de usar a ferramenta, seus dados poderiam ser conservados no Facebook. Esse é um ponto problemático, abre possibilidade para que as empresas transfiram dados para conservá-los a despeito dos objetivos originais. Isso ocorre, pois a solidariedade entre as empresas permite que ocorra a transferência e o compartilhamento dos dados pessoais pelos responsáveis. Pois a terceiros que, direta ou indiretamente, contribuam para a realização de seus tratamentos, é permitida a conservação para a finalidade inicial desses dados.

8.11 Aplicativos para controle do ciclo menstrual

Dentre os vários aplicativos desenvolvidos diariamente, uma nova tendência tem se mostrado particularmente preocupante⁵³. Os aplicativos que prometem a mulheres um maior controle sobre o ciclo menstrual e suas implicações no organismo têm acumulado um número significativo de dados sensíveis que estão sendo comercializados com empresas de vendas de dados.

As informações fornecidas pelas usuárias do aplicativo variam desde os dias de seu período menstrual até informações como a última vez e em que posição tiveram relações sexuais ou se estiveram doentes, quais sintomas tiveram e como se trataram. Estes dados são de extremo valor para empresas que anunciam produtos e serviços de saúde, como fabricantes de remédio ou seguradoras.

8.11.1 Análise do caso

O tratamento de dados pessoais é permitido quando necessário para atender aos interesses legítimos do responsável ou de terceiro, exceto no caso de prevalecerem interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for menor de idade. Os aplicativos de controle sobre o ciclo menstrual atuam claramente na intersecção apontada pelo inciso, sendo que o interesse das usuárias pela utilização e compartilhamento de seus dados sensíveis deve prevalecer ante o interesse do responsável. A finalidade do tratamento deve ser adequada e ostensiva, os sujeitos

⁵³ Fonte da notícia: <<https://www.nexojornal.com.br/expresso/2016/10/03/Os-aplicativos-sobre-os-ciclos-menstruais-e-a-exposi%C3%A7%C3%A3o-de-dados-pessoais-das-usu%C3%A1rias>> Acesso em: 03 de outubro de 2017.

ou categorias de sujeitos para os quais os dados podem ser comunicados e o âmbito de sua difusão. Já o tratamento de dados pessoais sensíveis, que fica proibido, exceto em casos nos quais haja o consentimento livre, inequívoco, informado, expresso e específico em quase todos os casos, com raras exceções. Dessa maneira, os aplicativos de controle do ciclo menstrual teriam de informar detalhadamente a suas usuárias cada possibilidade de tratamento dos dados que foram inseridos, inclusive as atividades de terceiros. Além disso, mesmo com o consentimento das mulheres, o tratamento de dados pessoais sensíveis deve contar com um modo de segurança mais robusto e tecnologicamente atualizado.

8.12 Vigilância estatal

Em 2013, ocorreram centenas de manifestações populares em todo o país. Iniciou-se com a organização de um movimento contra o aumento das tarifas do transporte público, mas ganhou proporções que extrapolaram em muito esse tópico. Naquela época, uma reportagem publicada no jornal O Estado de S.Paulo⁵⁴ revelou que a Agência Brasileira de Inteligência havia montado uma equipe para monitorar as organizações dos protestos no Facebook, Twitter, Instagram e até no WhatsApp, um aplicativo de mensagens que não possui interface pública, e que por isso requer uma quebra de sigilo de comunicação dos usuários.

8.12.1 Análise do caso

Esse tipo de ação não é permitida pela legislação brasileira e seria como a prática de um grampo telefônico sem ordem judicial, uma violação do artigo 5, inciso XII da Constituição Federal e da lei 9.296/96, que regulamenta esta questão. Além disso, o monitoramento de dados pessoais que estejam em acesso público não dá o direito a forças policiais ou de inteligência de processar, analisar e autorizar operações com base neles, pois, mesmo estando em acesso público, os titulares destes dados deveriam fornecer seu consentimento para que seus dados fossem assim utilizados.

⁵⁴Fontes da notícia: <<http://www1.folha.uol.com.br/poder/2015/08/1669267-equipe-da-abin-a-servico-da-rio-2016-vai-monitorar-protesto-contradilma.shtml>>; <<http://sao-paulo.estadao.com.br/noticias/geral,abin-monta-rede-para-monitorar-internet,1044500>> Acesso em: 03 de outubro de 2017.

CONSIDERAÇÕES FINAIS

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

A sociedade da informação e do consumo proporciona uma nova realidade tecnológica que, apesar de trazerem avanços, também carrega consigo novas situações de violação da vida privada, tais como a coleta, o tratamento e o compartilhamento indevidos dos dados pessoais dos indivíduos, sobretudo no meio digital. Não restam dúvidas de que tal circunstância ameaça os interesses dos cidadãos e do próprio Estado. A ausência de regulamentação quanto à coleta e o tratamento dos dados pessoais, ou a sua disposição insuficiente, tanto pode favorecer o seu uso como uma ferramenta totalitária por parte dos governos, quanto pode ser manejada pela iniciativa privada no intuito de padronizar e classificar os indivíduos em prol do estrito consumo. Este novo direito fundamental à proteção dos dados pessoais já vem sendo paulatinamente reconhecido no direito comparado, a exemplo do que vem ocorrendo no continente europeu e nos Estados Unidos, fruto da preocupação com o dano em potencial que a exposição das informações pessoais pode causar aos direitos e garantias fundamentais dos indivíduos.

O direito brasileiro já vem acompanhando este movimento. Com o surgimento da Lei nº 12.965/14, o Brasil sanciona sua primeira norma legal destinada à proteção dos direitos dos usuários da rede mundial de computadores, que fora regulamentada por meio do Decreto nº 8.771/16, estabelecendo diretrizes sobre padrões de segurança na atuação dos provedores de conexão de internet.⁹⁷ Não se pode deixar de reconhecer a tentativa louvável do Brasil no sentido de proteger este novo direito fundamental, estruturado a partir das necessidades da sociedade moderna.

Entretanto, também não se pode desconsiderar que a dinâmica complexa da sociedade da informação exige um aperfeiçoamento constante dos institutos legais, de modo a acompanhar as mudanças sociais. O surgimento de uma norma legal não induz, necessariamente, à sua plena efetivação. Os diplomas vigentes no direito brasileiro parecem não serem suficientes para se atribuir ao indivíduo o controle sobre os seus próprios dados pessoais, sobretudo porque a internet é uma tecnologia transnacional. Em tais normas não parece ter sido considerada as limitações territoriais, o custo inerente à implementação das ferramentas de segurança e, tampouco, a estrutura necessária para a fiscalização destas normas. Não se pode ainda traçar uma estatística sobre o cumprimento desta norma. O tema é muito recente e passou à pauta secundária diante da crise política e econômica enfrentada pelo país. Entretanto, o futuro é desafiador, mesmo com a vigência deste Decreto. Por fim, vale ressaltar que a privacidade é elemento fundamental para a liberdade de expressão, na medida em que certas mobilizações e articulações sociais e políticas requerem confiança entre os pares para que ocorram. Quando agentes ou instituições do Estado ou do governo empregam práticas de vigilância, eles limitam a livre comunicação de ideias porque constroem o livre pensamento e coíbem qualquer tipo de questionamento a eventuais abusos de diversos atores ou até mesmo o questionamento da ordem vigente. A dinâmica social é bastante ampla e complexa para ser solucionada através de uma legislação nacional, desconsiderando um arranjo internacional mais eficaz. É necessário, portanto, garantir o direito à privacidade para que o direito à liberdade de expressão possa ser pleno.

A dinâmica social é bastante ampla e complexa para ser solucionada através de uma legislação nacional. Uma solução mais eficaz parece emergir para além das fronteiras do Estado, através de arranjos internacionais mais eficazes que vinculem o maior número possível de nações, o que melhor se compatibilizaria com o caráter transnacional da internet. A doutrina nacional também precisa assumir seu papel na difusão deste conhecimento. É importante um esforço pela consolidação de uma dogmática onde se possam construir reflexões que fundamentarão uma base sólida para auxiliar o Poder Judiciário na aplicação atual e futura deste direito, bem como orientar a atuação do Estado em prol da implementação de políticas públicas eficazes neste sentido. O papel da sociedade civil também é fundamental neste

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

REFERÊNCIAS

AKERKAR, R. **Big data computing**. Boca Raton: Taylor & Francis Group, LLC, 2014.

BASTOS, C. R; MARTINS, Ives Gandra. **Comentários à Constituição do Brasil**. Vol. 2, São Paulo: Saraiva, 1989, p. 63.

BEAL, A. **O sistema de informação como estratégia empresarial**. São Paulo: Atlas, 2001.

_____. **Gestão Estratégica da Informação**: como transformar a informação e tecnologia da informação em fatores de crescimento e alto desempenho nas Organizações. São Paulo: Atlas, 2004.

BESSA, L. Sistema Nacional de Defesa do Consumidor. In: BENJAMIM, Antônio Herman V.; MARQUES, Cláudia Lima; BESSA, Leonardo Roscoe. **Manual de direito do consumidor**. São Paulo: Revista dos Tribunais, 2008.

BOBBIO, N. **A era dos direitos**. Rio de Janeiro: Campus, 1992.

BRASIL. Conselho da Justiça Federal. **VI Jornada de Direito Civil**. Disponível em: <<http://www.cjf.jus.br/cjf/CEJ-Coedi/jornadas-cej/enunciados-vi-jornada/view>> Acesso em: 2 de out. 2017

_____. Constituição. **Constituição da República Federativa do Brasil**. Diário Oficial da União, 5 out. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 2 de out. 2017

_____. Lei nº 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: 2 de out. 2017

_____. Lei nº 8.078, de 11 de setembro de 1990. **Dispõe sobre a proteção do consumidor e dá outras providências**. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm> Acesso em: 2 de out. 2017

_____. Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 2 de out. 2017

CANOTILHO, J J G. **Constituição da República Portuguesa Anotada**. 4. Ed. Coimbra: Editora Coimbra, 2007.

CASTELLS, M. **A sociedade em rede**. São Paulo: Paz e Terra, 1999

CASTELLS, M. **A sociedade em rede a era da informação: economia, sociedade e cultura**. 5.ed. São Paulo: Paz e Terra, 2001. v.1.

CASTRO, C. S. **O direito a autodeterminação informativa e os novos desafios gerado pelo direito à liberdade e a segurança no pós 11 de setembro**. Coimbra: Coimbra, Vol II. 2015.

CATALA, P. *Ebauche d'une théorie juridique de l'information*, in: Informatica e Diritto, ano IX, jan-apr. 1983. Disponível em: <http://www.ittig.cnr.it/EditoriaServizi/AttivitaEditoriale/InformaticaEDiritto/1983_01_015-031_Catala.pdf> Acesso em: 2 de out. 2017

CHIZZOTTI, A. **Pesquisa em ciências humanas e sociais**. São Paulo: Cortez, 1995.

COMER, D. E. **Interligação de redes com TCP/IP: princípios, protocolos e arquitetura**. Vol.1.5.ed. Rio de Janeiro: Elsevier, 2006.

CONESA, F. M. *Derecho a la intimidad, informática y Estado de Derecho*, Universidad de Valencia, Valencia, 1984.

COSTA JR., P. J.. **O Direito de Estar Só: Tutela Penal da Intimidade**. 4ª Ed. São Paulo: Revista dos Tribunais, 2007.

DARRELL. K.. *Issues in internet: society, technology, and the law*. 6. Ed. Boca Raton-FL. 2011.

DE LA CUEVA, P. L. M.. *El derecho a autodeterminacion informativa*. Madrid: Tecnos. 2013.

DIAS, G e VIEIRA, A. **Big Data: questões éticas e legais emergentes**. Revista da informação. Brasília, DF, v. 42 n. 2, p.174-184. 2013.

DIAZ, E. L. *El derecho al honor y el derecho a la intimidad*. Madrid. 2013.

DONEDA, D. **Privacidade e transparência no acesso à informação pública**. Zaragoza: Prensas Universitarias de Zaragoza, 2010. Disponível em: <<http://www.egov.ufsc.br/portal/sites/default/files/lefis11-09.pdf>>. Acesso em: 2 de out. 2017

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

DRUCKER, P. F. **Administrando para o futuro: os anos 90 e a virada do século.** São Paulo: Enio Matheus Guazzelli & Cia Ltda., 1992.

DRUMMOND, V. **Internet, privacidade e dados pessoais.** Rio de Janeiro: Lúmen Júris, 2003, p. 50.

EXAME. **Seu nome, CPF e endereço podem estar disponíveis neste site sem que você saiba.** Disponível em: <<http://exame.abril.com.br/tecnologia/noticias/seu-nome-cpf-e-endereco-completos-podem-estar-disponiveis-neste-site-sem-que-voce-saiba-disso>> Acesso em: 2 de out. 2017

FARIA, P. R. **A constituição Portuguesa anotada.** 2.ed. Coimbra. 2010.

FIGUEIREDO, N.M.A. **Método e metodologia na pesquisa científica.** 2a ed. São Caetanodo Sul, São Paulo, Yendis Editora, 2007.

FROTA, H. A. **A proteção da vida privada, da intimidade e do segredo no Direito Brasileiro Comparado.** Revista Jurídica Unijus. V.9, n. 11, Uberaba.

G1. **Entenda o caso Eduard Snowden.** 2013. Disponível em: <<http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>> Acesso em: 2 de out. 2017

GARSTKA, H. *Informationelle Selbstbestimmung und Datenschutz.* In: SCHULZKI-HADDOUTI, Christiane. *Bürgerrechte im Netz.* Bonn: Bundeszentrale für politische Bildung, 2003. p. 49.

GERMAN PARLIAMENT. *Federal Data Protection Act* Disponível na Internet via: <<http://www.bfd.bund.de>> Acesso em: 2 de out. 2017

GIL, A. C. **Como elaborar projetos de pesquisa.** 4. Ed. São Paulo: Atlas, 2002.

GREENWALD, G. **Sem lugar para se esconder: Edward Snowden, a NSA e aespionagem do governo americano.** Rio de Janeiro: Sextante, 2014.

HAUAISS, A. **Minidicionário Hauaiss.** 3a ed. Rio de Janeiro, Objetiva, 2008.

IG, Tecnologia. **'Tudo Sobre Todos': site vende dados pessoais e mostra até endereço no mapa.** Disponível em: <<http://tecnologia.ig.com.br/2015-07-25/tudo-sobre-todos-site-vende-dados-pessoais-e-mostra-ate-endereco-no-mapa.html>> Acesso em: 2 de out. 2017

LEMOS, A. **Cibercultura**: tecnologias e vida social na cultura contemporânea. 5. Ed. Porto Alegre: Sulina, 2010.

LÉVY, Pierre. O que é virtual?. Tradução Paulo Neves. São Paulo: Editora 34, 2011.

Ley 25.326/2000 cf. ARGENTINA. *Ley 25.326/2000 de proteccion de los datos personales*. Disponível em: <<http://www.jus.gob.ar/datos-personales.aspx>> Acesso em: 2 de out. 2017

Ley Federal de Protección de Datos Personales em Posesión de los Particulares cf. MEXICO. Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Publicada no Diário Oficial em 05.07.2010) Disponível em: <<http://www.ifai.org.mx/>> Acesso em: 2 de out. 2017.

Ley nº 1.682/01, parcialmente modificada pela ley nº 1969/2002 cf. PARAGUAY. Ley nº 1.682/01, que reglamenta la información de carácter privado. Disponível em: <http://www.leyes.com.py/todas_disposiciones/2001/leyes/ley_1682_01.php> Acesso em: 2 de out. 2017.

Ley nº 18.331/2008, de protección de datos personales y acción de habeas data (Publicada D.O. 18 ago/008 - Nº 27549). Disponível em: <<http://www.datospersonales.gub.uy/sitio/>> Acesso em: 2 de out. 2017

Ley nº 19.628/99 cf. CHILE. Ley nº 19.628 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: 2 de out. 2017.

MANNINO, V. **Projeto, desenvolvimento de aplicações & administração de banco de dados**. 3ª ed. São Paulo: McGraw-Hill, 2008.

MARÇULA, M. **Informática**: Conceitos e aplicações. 3. E. São Paulo. Erica, 2008.

MARION, A. *Informationelle selbstbestimmung*. Deutsch: Nomos. 2005.

MARQUES, G; MARTNS, L. **Direito a Informática**. Coimbra: Almeidina, 2000.

MCKINSEY GLOBAL INSTITUTE, *Big data: The next frontier for innovation, competition and productivity*. June 2011.

MENDES, G. **Direitos Fundamentais e Controle de Constitucionalidade**, São Paulo: Saraiva, 2012.

MINAYO, M. C. S. (Org.). **Pesquisa social**: teoria, método e criatividade. Petrópolis: Vozes, 2003.

MISNISTERIO PUBLICO. Pensando Direito – Debate sobre Proteção de Dados Pessoais. 2015. Disponível em: <<http://pensando.mj.gov.br/dadospessoais/>> Acesso em: 2 de out. 2017

MORAES, A. F. **Segurança em Redes**: fundamentos. 1ed. São Paulo: Érica, 2010.

MURILLO, P. L. **El Derecho A La Autodeterminación Informativa**. Tecnos, Madrid, 1990.

NONAKA, I.; TAKEUCHI, H. Criação do conhecimento na empresa: como as empresas japonesas geram a dinâmica da inovação. Rio de Janeiro: Campus, 1997.

OLIVEIRA, S. L. **Metodologia Científica Aplicada ao Direito**. São Paulo: Thomson, 2002.

ORGANIZAÇÃO MUNDIAL DA PROPRIEDADE INTELECTUAL (OMPI). Convenção de estabelecimento da Organização Mundial da Propriedade Intelectual. Estocolmo, 14 de julho de 1967.

ORWELL, G. **1984**. 29ª ed. São Paulo: Ed. Companhia Editora Nacional, 2005.

PÁDUA, E. M. M. de. **O processo de pesquisa**. In: _____. Metodologia da pesquisa: abordagem teórico-prática. Campinas: Papirus, 1997. p. 29 – 89. (Coleção Práxis).

PEREIRA, M.C.. **Direito à Intimidade na Internet** . Curitiba: Juruá Editora, 2003.

PEREZ LUÑO, A.E. *Ensayos de Informática Jurídica*. México: Biblioteca de Ética, Filosofía del Derecho y Política, 1996, p. 35.

PORTUGAL. Lei. 67 de 26 de outubro de 1998. Disponível em: <https://www.cnpd.pt/bin/legis/nacional/lei_6798.htm > Acesso em: 2 de out. 2017

RAPOSO. V. L. **A vida num código de barras**. Coimbra: Coimbra, Ed., Vol. VI. 2010.

RESS, W. **Começando a segurança**. 2011. Disponível em: <<https://msdn.microsoft.com/ptbr/library/ff716605.aspx>> Acesso em: 2 de out. 2017.

RICHARDSON, R J. **Pesquisa social**: métodos e técnicas. 3. ed. São Paulo: Atlas, 1999.

RODOTA, S. **A vida na sociedade da vigilância a privacidade de hoje**. Rio de Janeiro: Renovar. 2008.

ROJAS, S. Z.. *La problemática entre el derecho al ovido y la libertad de prensa*. Nueva Época, n. 13. 2013. Disponível em:

<<https://dialnet.unirioja.es/servlet/articulo?codigo=4330379>> Acesso em:2 de out.2017

RULLI, A. J.; RULLI, A. N. **Direito ao esquecimento e o superinformacionismo**: apontamentos no Direito Brasileiro dentro do contexto da sociedade da informação. Revista Instituto de Direito Brasileir. n. 1., Lisboa, jan. 2012.

SATHI, A. *Big data analytics*: disruptive technologies for changing the game. IBM Corporation, 2012.

SENADO FEDERAL. Portal Atividade Legislativa, Projetos e Matérias Legislativas – Projeto de Lei 330/2011 - Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências. Disponível em : <http://www.senado.gov.br/atividade/materia/detalhes.asp?p_cod_mate=113947> Acesso em:2 de out.2017

SETZER, V. **Dado informação conhecimento e competência**. DataGramaZero: Revista de Ciência da Informação - n. zero, artigo 1, p. 1-17, dez, 1999.

SEVERINO, A. J. **Metodologia do trabalho científico**. 22. ed., São Paulo:Cortez, 2002.

SOARES, L. F. G., ET AL. **Redes de Computadores**: das LANs, MANs eWANs as Redes ATM. 2ed. Rio de Janeiro: Campus, 1995.

STAIR, R.; REYNOLDS, G. **Princípios de Sistemas de Informação**: uma abordagem gerencial. Rio de Janeiro: LTC, 2002.

STAIR, R. M. **Princípios de Sistemas de Informação**: uma abordagem gerencial. Trad. Maria Lúcia Iecker Vieira e Dalton Conde de Alencar. 2.ed. Rio de Janeiro: LTC Editora, 1998. p. 4.

SVEIBY, K. E. **A nova riqueza das organizações**. Rio de Janeiro: Campus, 1998.

TAURION, C. **Big data**. Rio de Janeiro: Brasport, 2013. ePUB.

VALDÉS, J. T.. *Derecho informático*. 2 ed. México: McGraw-Hill, 2006.

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

WACKS, R. *Personal information: privacy and the law*. Oxford: Clarendon Press, 1989

WARREN, S.D. BRANDEIS, L. D. S. *The Right to Privacy*. *Harvard Law Review*, Vol. 4, No. 5 (Dec. 15, 1890). Disponível em:<<http://www.english.illinois.edu/-people>>

/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf> Acesso em:2 de out.2017.

WATERS, N. *Privacy Exemptions in FOI Laws—An Unnecessary Barrier to Accountability* -Documento preparado para o Simpósio Internacional sobre a liberdade de Informação e Privacidade, Auckland, Nova Zelândia, 2002.

WEISER, M. *The Computer for the 21st Century*. vol. 265, no.3, 1991.

XIMENES, J. M. **Levantamento de dados na pesquisa em Direito**: a técnica da análise de conteúdo. Anais do XX Congresso Nacional do CONPEDI Tema: "A Ordem Jurídica Justa: um diálogo Euroamericano. 1ed.Florianópolis: Fundação Boiteux, 2011, v. 1, p. 7608-7622

ZAGOL, C; TIBIRIÇÁ, S. A. **Direito à Informação e Privacidade**: Equilíbrio Gestão e Conflitos. ETIC - Encontro de Iniciação Científica. Vol. 7, No 7. 2011. Disponível em:<<http://intertemas.unitoledo.br/revista/index.php/ETIC/article/view/3860/3620>> Acesso em: jun 2017.

ZANINI, L. E. A. **O Surgimento E O Desenvolvimento Do Right Of Privacy Nos Estados Unidos**. Revista Eletrônica da Faculdade de Direito de Franca, [S.l.], v. 9, n. 2, p. 110-132, dez. 2014.. Disponível em: <<http://www.revista.direitofranca.br/index.php/refdf/article/view/261>>. Acesso em:2 de out.2017

ZANON, J. C. **Direito à proteção dos dados pessoais**. Dissertação (Mestrado em Direito) - Pontifícia Universidade Católica de São Paulo, São Paulo, 2012.