GESTÃO JURÍDICA NA PROTEÇÃO DE DADOS PESSOAIS

Tassyara Onofre de Oliveira
Doutoranda no Programa de Pós-Graduação em Ciência da Informação da Universidade Federal da Paraíba. Mestra pelo Programa de Pós Graduação em Gestão nas Organizações Aprendentes na Universidade Federal da Paraíba. ORCID: https://orcid.org/0000-0003-4048-8322.
E-mail: tassyjp@gmail.com

Geovanna Cristina Falcão Soares Rodrigues
Doutora em Educação pelo Programa de Pós-Graduação em Educação da Universidade Federal da Paraíba. Pesquisadora vinculada à Rede Interdisciplinar de Estudos sobre Violências (RIEV). ORCID: https://orcid.org/0000-0001-9121-7421.
E-mail: geovannacristinaf@yahoo.com.br

Resumo: O aparelhamento tecnológico tem auxiliado e provocado mudanças na vida cotidiana. Novos caminhos e desafios são colocados à vida em sociedade, uma vez que esta tem como marca a informação e o conhecimento no universo digital. Na Rede são requisitados uma infinidade de dados pessoais, ao mesmo tempo em que as próprias pessoas expõem informações e formas de pensamentos (fotos, comentários) que são captadas pelos softwares a fim de traçar um perfil dos usuários. Esse contexto inovador, trouxe desafios ao sistema legal no que se refere a regulação jurídica de acesso e compartilhamento de informações pessoais no ciberespaço. A proposta desse artigo foi discutir sobre a garantia de proteção aos dados pessoais a partir de sua dimensão objetiva e subjetiva presente no sistema de direitos fundamentais de acordo com a legislação brasileira.

Palavras-chave: Gestão da informação. Gestão de dados pessoais. Ordenamento jurídico brasileiro.

LEGAL MANAGEMENT IN THE PROTECTION OF PERSONAL DATA

Abstract: Technological equipment has helped and provoked changes in everyday life. New ways and challenges are brought to life in society, as it has as its mark information and knowledge in the digital universe. In the Network are requested a multitude of personal data, at the same time as people themselves expose information and thought forms (photos, comments) that are captured by the software in order to draw a profile of users. This innovative context has brought challenges to the legal system regarding the legal regulation of access and sharing of personal information in cyberspace. The purpose of this article was to discuss the protection of personal data from its objective and subjective dimension present in the fundamental rights system in accordance with Brazilian law.
Keywords: Information management. Management of personal data. Brazilian legal system.

Artigo recebido em: 02/10/2019

Aceito para publicação em: 29/11/2019

Introdução

A sociedade atual configura-se por ser globalizada e tecnológica, cuja marca é a informação e o conhecimento virtualizado. Essa "nova era" tem sido nomeada de Sociedade da Informação, termo difundido e conceituado por Machlup (1962)[1] ou de modo mais amplo, como afirma Castells (1999) vive-se na 'Sociedade em Rede', onde não há limites para que a informação possa alcançar seus objetivos (CASTELLS, 1999). Para definir a Sociedade em Rede, Castells (1999), destaca o contexto de expansão e reestruturação do capitalismo e apresenta como marco as décadas de 70/80 (CASTELLS, 1999)[2] com o aparecimento da Internet, e seu universo virtual, de modo mais presente no cotidiano das pessoas.

Para Lévy (2011) é evidente a influência do ambiente virtual em todas as esferas da sociedade, categorizando transformações nunca antes vistas no curso histórico da humanidade. A 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)

O mundo cada vez mais se digitaliza e gera conteúdo digital. Diversas são as possibilidades de comunicação e acesso ao conhecimento, através de conexões e saberes compartilhados, que possibilitam inúmeras direções e a difusão do conhecimento e da informação. É importante reconhecer o papel que, nos ambientes virtuais, a informação desempenha na sociedade, suas implicações e a necessidade de discutir maneiras de lidar com esse fato, uma vez que o momento atual é caracterizado por mudanças influenciadas cada vez mais pelos avanços tecnológicos.

A informação sempre foi valorizada na história da 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 atual é o *Google Flu Trends*[3] que pode detectar e prevenir contra surtos de gripe ou o *Google Dengue Trends*[4] que tem a função de alertar sobre os principais surtos de dengue no mundo, um problema presente em nosso país.

Ademais, a sociedade passa por transformações onde não existe mais anonimato em meio à multidão. Os tradicionais locais públicos como praças, ruas, parques, aeroportos e centros comerciais, assim como as próprias pessoas, são

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).

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, online).

4 "Google Dengue Trends are no longer publishing current estimates of Flu and Dengue fever based on search patterns" (GOOGLE, online).

submetidos cada vez mais a um acompanhamento efetivo de suas ações. As câmeras de vigilância, por exemplo, são utilizadas para o monitoramento do trânsito, prevenção e elucidação de crimes e estão espalhadas ao longo de avenidas, casas e no interior de estabelecimentos comerciais e institucionais, afim de coletar o máximo de informação. Contudo, 'para que' e 'para quem' estas informações estão sendo coletadas? Para nossa proteção ou para nosso controle?

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 que identificam aspectos da sua personalidade e de seu comportamento com a finalidade de traçar um perfil virtual que contém seus pontos de interesse e até mesmo inferem possibilidades futuras. Assim, na sociedade da informação a geração de dados é cada vez maior e mais acelerada.

Inúmeros são os dados pessoais que podem ser armazenados sem nosso conhecimento e sem nenhuma garantia de que serão utilizadas de maneira ética ou de uma forma que concordemos. O conhecimento que é gerado da informação de nossos dados pessoais são ativos intangíveis e abundantes, sendo assim, o conhecimento gerado pela coleta de informações pode ser usado por pessoas e empresas sem que se reduza o estoque. O armazenamento e análise de todo e qualquer dado na Internet pode ajudar a traçar comportamentos e tendências. Através do processamento de dados abre-se um gigantesco potencial de enriquecimento.

A realidade virtual passou a ser tão presente no cotidiano dos indivíduos e da sociedade que resultou no conceito de 'ubiquidade dos meios informáticos' ou 'computação pervasiva' (*Ubiquitous Computing* ou *ubicomp)*. Tal conceito foi citado pela primeira vez por Mark Weiser (p. 94, 1991)[5] e descreve, justamente, a onipresença da informática no cotidiano das pessoas, através de aparelhos de *smartphones,* a Internet em nuvem, a Internet das coisas (IoT) entre outros artefatos tecnológicos. Com todos esses novos recursos de comunicação, facilitando a vida com a tecnologia e a circulação de conhecimento e informação, surgiram, conjuntamente, um maior controle social, uma exposição indesejada dos dados e da espontaneidade individual (intimidade, imagem, dados pessoais).

Em nenhum outro espaço a vigilância é tão permanente como na Internet, tendo as redes digitais como seu símbolo maior. 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.* Nós somos os nossos dados, através deles podem nos definir e nos classificar, além de nos proporcionar acessos a produtos e serviços, privados e públicos, que muitas vezes nem desejamos.

Desse modo, a segurança da informação torna-se importante para todos os usuários das Redes. O objetivo não é de proteger os dados apenas, mas sim, o titular desses dados, defendê-lo de organizações sejam elas públicas ou privadas. Tendo em vista que os dados pessoais se constituem intermediários entre a pessoa e a sociedade. Um dos casos de invasão de privacidade que ganhou repercussão mundial foi o 'Caso Snowden'[6], que revelou ocorrência de espionagem por parte do governo dos EUA. O fato gerou crise para o governo Obama perante todo o mundo e abalou a confiança de todos os cidadãos americanos que se viram expostos por um Estado que ao invés de proteger a integridade e o sigilo das

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

6 GREENWALD, 2014.

informações que circulam pelos meios tecnológicos, a viola.

No Brasil, o Departamento Estatual de Trânsito (DETRAN) do Rio Grande do Norte vazou informações pessoais de 70 milhões de brasileiros que possuem a Carteira Nacional de Habilitação (CNH) no país. As informações expostas na Internet continham endereço residencial, números de telefone, sexo, data de nascimento, CPF e carteira de identidade, além da foto do documento. Em nota o órgão reconheceu a falha no sistema de segurança referente ao registro das carteiras de motorista e avisava que o erro fora corrigido (NAKAGAWA, 2019).

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, fazendo surgir novos conceitos, transformações e discursões. 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.

Segundo Castells (2001, p. 59), ao citar a primeira Lei de Kranzberg, "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. Desse modo, a proteção de dados pessoais surge para a prevenção contra os potenciais riscos que podem ser causados às pessoas, sendo eles originados do tratamento e o uso indevido dos dados por agentes humanos, seja no setor público ou privado.

A Sociedade em Rede exibe uma visão de Estado e de empresas privadas que vigiam, cada vez mais e com mais facilidade, as pessoas, seja com o amparo da ubiquidade, seja pela utilização das mais diversas tecnologias, com um a enfoque nos *smartphones*. Esta realidade provoca um debate sobre privacidade na rede e acende o alerta de um contexto como um *Big Brother*[7], que tudo quer saber, controlar e ver. Desse modo, 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.

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 subjetiva, o qual depende muito de condições particulares como o tempo, classe, condição social, econômica e outros fatores subjetivos. Dito de outra forma, a proteção de dados *é qualitativamente diferente do tradicional direito à privacidade e a alavanca dessas mudanças é exatamente o uso intenso e inovador das tecnologias*, 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 com as informações pessoais dos usuários.

Portanto, 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, por outro a coleta de informações sobre dados pessoais que anteriormente eram particulares, agora estão soltos na rede sem nenhuma autorização dos seus reais titulares. Porém, a gestão jurídica e o controle de processos tornam-

7 Expressão citada por George Orwell em sua obra 1984.

se indispensáveis para um equilibro entre todos os sujeitos nessa sociedade tão atual e inovadora, uma vez que os dados que circulam na rede são universais e os impactos também.

O âmbito de proteção dos direitos fundamentais

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.

Assim, a proteção a informação encontra-se presente em diversas áreas jurídicas: no direito penal há proteção contra injuria ou difamação, no direito comercial é segurado o sigilo empresarial e propriedade industrial, já no direito constitucional são garantidos os direitos fundamentais como a liberdade de expressão e de impressa. Tratam de normas de direito tão antigas, mas que já reconheciam a importância de proteger a informação, na vida da sociedade e dos indivíduos.

Na sociedade contemporânea – caracterizada exatamente pelo fluxo intenso de informação a partir de uma moderna estrutura de comunicação e informação – os 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 em dados raciais ou de imigrantes, prática conhecida como *racial profiling*[8];

(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"[9],

(iii) 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 em lista de terroristas poderiam construir uma limitação à liberdade de ir e vir[10] e

(v) reuniões em espaços públicos podem ser afetadas se os seus participantes forem filmados e registrados sem justificativa.

Percebe-se que o processamento e utilização de dados afetam não apenas os direitos fundamentais que expressamente regulam o fenômeno da informação, mas afetam, na realidade, todo o sistema de direitos fundamentais que podem ser influenciados, positiva ou negativamente, por esse fenômeno. Esses exemplos 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

8 Prática de 'Perfilamento social' (GELLERT *et al.*, 2013).

9 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.

10 As "*no fly list*" são listas mantidas pelo governo Americano onde até crianças são impedidas de embarcar por terem seus nomes incluídos em 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

e a comunicação social. Assim, os sistemas informáticos transformam o mundo do trabalho, da administração pública e privada e do mercado. Com isso, sem o sistema de direitos fundamentais se torna impossível o livre exercício de qualquer trabalho, ofício ou profissão, a livre expressão da atividade intelectual, artística, científica e de comunicação.

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

No âmbito de proteção, o direito fundamental à proteção dos dados regula uma ordem de informação e comunicação, e, pela sua essência multidimensional, 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 residiu menos nos dados em si, e mais, nos processos de coleta, armazenamento, utilização e transferência, a partir dos quais são extraídas informações pessoais a serem utilizadas em um determinado contexto para determinados fins. A proteção constitucional entra em ação se a informação coletada for usada para uma finalidade que cause riscos ou seja considerado ilícitos *a priori* (como é o caso dos bancos de dados criados a fins discriminatórios). Assim, somente uma análise que envolve: (i) o contexto do uso das informações (ou das hipóteses previstas para a sua utilização), (ii) o conteúdo da informação, (iii) a finalidade de sua utilização e (iv) os riscos aos cidadãos é que pode determinar a legitimidade de ação de tratamento de dados e informações pessoais.

Ademais, o bem jurídico protegido por esse direito é duplo, pois 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). Compreende-se a informação como direito duplo seja o entendimento mais apropriado, por reconhecer que o processamento de dados pessoais influencia o sistema de direitos fundamentais na sua totalidade.

Em consonância, o âmbito de proteção do direito fundamental à proteção dos dados pessoais pode ser concebido em uma dupla dimensão, conforme Pieroth e Schlink (2005, p. 17):

> 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.

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.

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, liberdade e privacidade, não sujeitas a intervenções estatais. No caso de violação de direito subjetivo, enseja que a intervenção cesse, e, em caso de uma provável violação, o direito fundamental possibilita a tomada de atitudes

preventivas para não ocorrência da respectiva 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), afirmam que 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 ao próprio sujeito, influenciam, assim, a sua esfera de direitos e somente o titular pode determinar a extensão de circulação de seus dados na sociedade.

Contudo, 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: (i) 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 (ii) 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. Já 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 tem a ver com o contexto da relação trabalhista.

Outro exemplo envolve os bancos de dados da Bolsa Família[11]. 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.

Percebe-se que, em regra, prevalece a autodeterminação do titular sobre os dados pessoais, salvo direito de terceiros ou interesse público predominante previsto 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, no direito

11 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 (CAIXA, online).

brasileiro um núcleo fundamental desse direito à luz do conceito de que nenhum indivíduo deve ser submetido a uma coleta, processamento e circulação de dados pessoais de maneira ilimitada.

Ao mesmo tempo em que o direito fundamental à proteção de dados atribui ao indivíduo um espaço de liberdade, ele retira do Estado objetivamente 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 possuem também um conteúdo objetivo, para além do seu significado de direito de defesa subjetiva.

Na **dimensão objetiva** Mendes (2012, p. 469), afirma 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 objetivamente 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 pressupõem a ação positiva do Estado, sem a qual o direito perderia a sua eficácia. Já no direito fundamental à proteção de dados, se sobressai a esses dois tipos de ação.

No Brasil, a partir de agosto de 2020, entrará em vigor a Lei 13.709/18 – Lei Geral de Proteção de Dados Pessoais (LGPD) que em seu Artigo 1º:

> dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

De modo geral a Lei altera o Marco Civil da Internet e vem garantir transparência na proteção de dados pessoais, incluindo a proteção e privacidade de dados digitais. Por dados pessoais entende-se a " informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018). A referida Lei está dividida em dez capítulos que abrangem: o tratamento de dados pessoais; os direitos do titular; o tratamento de dados pessoais pelo poder público; a transferência internacional de dados, os agentes, a segurança e as boas práticas e a fiscalização. Incluem ainda capítulos destinados a Autoridade Nacional de Proteção de Dados (ANPD) e o conselho nacional de proteção de dados pessoais e da privacidade.

Considerações finais

Na Internet a geração de dados é cada vez maior e mais acelerada, o que constata o papel fundamental que a informação já exerce na Sociedade em Rede. Concomitantemente o mundo passa por mudanças de paradigma com relação à privacidade e proteção de dados pessoais. Na sociedade da informação, o direito *à* privacidade voltou-se para o risco em que se encontram milhares de cidadãos cujos dados pessoais são diariamente coletados, processados por órgãos estatais e privados, com o auxílio de modernas tecnologias.

Percebe-se que a privacidade e o controle na Internet estão diariamente em confronto, tornam-se, nesse universo, figuras antagônicas. 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. Reforça-se que não é a tecnologia em si que causa problemas de privacidade, mas sim as decisões que tomamos em relação ao uso dos meios tecnológicos. A sociedade da informação poderá obter vantagens dentro do desenvolvimento tecnológico quando acompanhado pelas orientações advindas de

gestão jurídica de privacidade, a qual visa garantir ao titular dos dados pessoais a autonomia das suas escolhas, como também, a sua dignidade e a tutela de personalidade.

A proteção dos dados pessoais é 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. Entendemos que a gestão jurídica dos dados pessoais terá êxito quando houver equilíbrio das assimetrias de poder sobre a informação pessoal, existente entre o titular dos dados pessoais, e aqueles que os usam e compartilham. As reflexões propostas neste artigo visaram não somente proteger o cidadão, como também fomentar uma sociedade e um mercado movido pela transparência dos dados coletivos que se configura pertinente a uma Sociedade em Rede.

Buscou-se refletir a partir do equilíbrio entre o direito a proteção dos dados pessoais ao mesmo tempo em que se defende a participação dos indivíduos no processo comunicativo. Cabe ao Estado proteger por meio das leis vigentes e aos legisladores atualizar a legislação tendo em vista a garantia da integridade moral dos indivíduos bem como a proteção da liberdade em sentido amplo.

Portanto, no que tange aos direitos de proteção a informação defendeu-se a execução e a implementação de leis de proteção aos dados pessoais que permitam ao cidadão ter uma melhor gestão sobre como suas informações são utilizadas por organizações, empresas e pelo próprio governo. Que tenha por objetivo estabelecer padrões mínimos a serem seguidos quando ocorrer o uso de um dado pessoal, que discorra sobre os limites acerca da utilização dos dados para finalidades específicas, que crie um ambiente seguro de modo a garantir aos cidadãos protagonismo nas decisões sobre a utilização de seus dados, ao mesmo tempo em que apresente a necessidade de campanhas educativas por parte do governo para que as pessoas aprendam a gerir com responsabilidade suas informações na Rede.

Referências

BRASIL. **Lei nº 13.709**. Presidência da República. Brasília, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 01 out. 2019.

CAIXA. **Bolsa Família.** Site da Caixa Econômica Federal, online. Disponível em: http://www.caixa.gov.br/programas-sociais/bolsa-familia/Paginas/default.aspx Acesso em: 03 ago. 2019.

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

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

GELLERT, Raphael; VRIES, Katja de; HERT, Paul de; GUTWIRTH, Serge. A Comparative Analysis of Anti-Discrimination and Data Protection Legislations. *In:* CUSTERS, Bart; CALDERS, Toon; SCHERMER, Bart; ZARSKY, Tal (ed.) **Discrimination and Privacy in the Information Society:** Data Mining and Profiling in Large Databases, Berlin: Springer-Verlag, 2013 Disponível em: encurtador.com.br/epHY6. Acesso em: 01 out. 2019.

GOOGLE. **Google Dengue Trends**. Online. Disponível em: https://www.google.org/flutrends/about/. Acesso em: 01 out. 2019.

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

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

MACHLUP, Fritz. **The Production and Distribution of Knowledge in The US Princeton**, N.J. Princ. Univ. Press, 1962.

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

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

NAKAGAWA, Liliane. **Detran vaza dados pessoais de quase 70 milhões de brasileiros**. Olhar digital, 2019. Disponível em: https://olhardigital.com.br/noticia/-exclusivo-detran-vaza-dados-pessoais-de-quase-70-milhoes-de-brasileiros/91308. Acesso em: 01 out. 2019.

ORWELL, George. **1984**. São Paulo: Companhia das Letras, 2009.

PIEROTH, Bodo; SCHLINK, Bernhard. **Direitos fundamentais**. Traduzido por Antonio Francisco de Sousa e Antonio Franco. São Paulo: Saraiva, 2012.

REVISTAGALILEU. **Google pode ajudar no controle da gripe**. Revista Galileu, online. Disponível: http://revistagalileu.globo.com/revista/common/0,,emi288897-17770,00-google+pode+ajudar+no+controle+da+gripe.html. Acesso em: 01 out. 2019.

WEISER, Mark. **The Computer for the 21st Century**. v. 265, n.3, p. 94-104. Setembro.1991. Disponível em: https://www.ics.uci.edu/~corps/phaseii/Weiser-Computer21stCentury-SciAm.pdf . Acesso em: 01 out. 2019.