

**ESCOLA DA MAGISTRATURA DO ESTADO DO PARANÁ
XXXIV CURSO DE PREPARAÇÃO À MAGISTRATURA
NÚCLEO CURITIBA**

MURILO EULLER CATUZO

**A PROTEÇÃO DOS DADOS PESSOAIS NO CONTEXTO DA SOCIEDADE DA
INFORMAÇÃO**

**CURITIBA
2016**

MURILO EULLER CATUZO

**A PROTEÇÃO DOS DADOS PESSOAIS NO CONTEXTO DA SOCIEDADE DA
INFORMAÇÃO**

Monografia apresentada como requisito parcial para conclusão do Curso de Preparação à Magistratura em nível de Especialização. Escola da Magistratura do Paraná.

Orientador: Prof. Dr. Antônio Carlos Efig

**CURITIBA
2016**

TERMO DE APROVAÇÃO

MURILO EULLER CATUZO

A PROTEÇÃO DOS DADOS PESSOAIS NO CONTEXTO DA SOCIEDADE DA INFORMAÇÃO

Monografia aprovada como requisito parcial para conclusão do Curso de Preparação à Magistratura em nível de Especialização, Escola da Magistratura do Paraná, Núcleo de Curitiba, pela seguinte banca examinadora.

Orientador: Prof. Dr. Antônio Carlos Efig

Avaliador: _____

Avaliador: _____

Curitiba, 31 de outubro de 2016.

SUMÁRIO

1 INTRODUÇÃO	6
2 A SOCIEDADE DA INFORMAÇÃO: CARACTERIZAÇÃO E REFLEXOS JURÍDICOS.....	8
3 A PROTEÇÃO DOS DADOS PESSOAIS NA LEGISLAÇÃO BRASILEIRA	16
3.1 A PROTEÇÃO CONSTITUCIONAL DOS DADOS PESSOAIS.....	17
3.2 – A PROTEÇÃO INFRACONSTITUCIONAL AOS DADOS PESSOAIS	25
4 ANÁLISE SISTÊMICA DA PROTEÇÃO JURÍDICA AOS DADOS PESSOAIS E A SUA APLICAÇÃO PELOS TRIBUNAIS	35
5 CONCLUSÃO	41
REFERÊNCIAS.....	43

RESUMO

Sob o contexto da sociedade da informação, o presente trabalho objetiva analisar a exposição dos dados pessoais em meio eletrônico e quais instrumentos legais estão disponíveis à sua proteção ante os riscos inerentes a esse recorte social. À vista disso e a partir de um exame sistêmico de registros estatísticos e da bibliografia pertinente ao tema, faz-se, de início, a caracterização da sociedade da informação e se apontam quais são seus reflexos jurídicos. Em seguida, apuram-se quais diplomas legislativos brasileiros possuem disposições direcionadas à proteção de dados pessoais. Tendo por base a Constituição Federal, verifica-se que a proteção aos dados pessoais se mostra imprescindível à proteção do consumidor e configura uma nova dimensão ao direito fundamental à privacidade. Em relação à proteção infraconstitucional, a proteção jurídica aos dados pessoais encontra amparo no Código de Defesa do Consumidor, no Decreto n. 7.962/2013 e na Lei n. 12.964/2014, que instituiu o Marco Civil da Internet. Diante desse panorama legal, constata-se a existência de direitos básicos e princípios que regulamentam a gestão dos dados pessoais no contexto da sociedade informação, uma vez que esses diplomas contam com disposições normativas aptas a definir os limites da gestão dos dados pessoais. Nota-se, por fim, que a proteção jurídica aos dados pessoais no contexto da sociedade da informação é sistêmica e complexa, já que, para ser efetiva, deve ser feita a partir de um dever jurídico de cooperação entre o titular dos dados e seu gestor.

Palavras-chave: Sociedade da Informação. Dados Pessoais. Constituição Federal. Código de Defesa do Consumidor. Decreto n. 7.962/2013. Marco Civil da Internet. Privacidade. Boa-fé.

1 INTRODUÇÃO

A crescente utilização de novas tecnologias, nos últimos tempos, em muito mudou as relações sociais. Além de facilitar a comunicação entre pares, o ininterrupto desenvolvimento da indústria tecnológica estimula cada vez mais pessoas à inclusão digital, que, para poder tornar os interlocutores identificáveis entre si, exige, por consequência, a constante disponibilização de dados pessoais.

A esse novo paradigma de dinamicidade social se dá o nome de sociedade da informação, cujo pressuposto é a gestão de registros imateriais por meio de mecanismos tecnológicos que impulsionam a articulação social.

No entanto, embora esse novo recorte sociológico se apresente extremamente benéfico à coletividade, é importante mencionar que essa nova estrutura social também pode ser muito nociva aos cidadãos, pois, em nome da facilidade de acesso aos mais diversos bens e serviços e comodidade trazida por esse novo contexto, nem sempre a segurança dos sujeitos é tratada da maneira necessária à eliminação ou suavização dos riscos inerentes a essa experiência digital.

Em razão disso, destaca-se que o uso indiscriminado dessas novas ferramentas tecnológicas pode aumentar, e muito, a vulnerabilidade do cidadão-consumidor, pois, por conta da intangibilidade do meio, o sujeito pode perder o total controle sobre o fluxo informacional disponibilizado.

Nota-se, portanto, que o contexto da sociedade da informação catalisa o fluxo de dados pessoais, motivo pelo qual se torna relevante conhecer os limites de atuação dos bancos de dados, especialmente no que concerne à salvaguarda, tratamento e gestão dessas informações.

Diante desse cenário e tendo por base os referenciais legislativo e teórico-bibliográfico analisados por um método dialético-dedutivo, propõe-se com esse trabalho identificar com quais fundamentos se dá, no Brasil, a proteção jurídica dos dados pessoais no contexto da sociedade da informação.

Para tanto, destaca-se, de início, o que é a sociedade da informação e qual a sua amplitude, o que se faz por meio da análise de dados estatísticos oficiais. Na sequência, tendo por aparato a hierarquia do conteúdo legislado, faz-se uma análise detida do ordenamento jurídico no que se refere à proteção dos dados pessoais. Por

fim, verifica-se, por meio da abordagem de uma hermenêutica sistêmica, em que nível está a proteção jurídica dos dados pessoais e como esse parâmetro de proteção tem sido entendido e aplicado pelos Tribunais.

2 A SOCIEDADE DA INFORMAÇÃO: CARACTERIZAÇÃO E REFLEXOS JURÍDICOS

Ainda que se parta de uma análise empírica do entorno social, não restam dúvidas de que a sociedade, em seus diferentes aspectos, em muito se modificou nos últimos anos, sobretudo ao se considerar o crescente e constante processo de informatização das relações sociais, o qual, obviamente, alterou e até mesmo intensificou o modo de conexão das pessoas entre e si e com os demais elementos e fatores sociais.

Para não restringir essa contextualização a uma simples e óbvia constatação fática, destaca-se, com base em dados estatísticos oficiais, que no Brasil, no período de 2005 a 2011, o número de pessoas que passaram a ter acesso à internet aumentou de 20,9% para 46,5% da população, o que retrata um universo de 77,7 milhões de pessoas com idade superior a 10 anos de idade.¹

Em ratificação a números cada vez mais significativos, nota-se, a partir da análise de dados mais recentes, que a inclusão digital dos brasileiros continua em ininterrupta ascensão, haja vista a facilitação ao acesso de meios de rápida comunicação.

Nesse viés, ao que consta da pesquisa realizada pelo Instituto Brasileiro de Geografia e Estatística no ano de 2014, cerca de 54,4% da população nacional se conectaram à internet durante aquele ano, o que corresponde a aproximadamente 95,4 milhões de pessoas com 10 anos ou mais.²

Diante desse amplo contexto, ressalta-se, segundo a referida pesquisa (2016, p. 23), que a internet, durante aquele período, fora utilizada para diversas funções, dentre as quais se destacam a participação em redes sociais e profissionais, a aquisição ou venda de bens e serviços e a utilização de serviços bancários.

¹ MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO. Instituto Brasileiro de Geografia e Estatística (IBGE). Pesquisa Nacional por Amostra de Domicílios (PNAD 2011): acesso à internet e posse de telefone móvel celular para uso pessoal. Rio de Janeiro, 2013. Disponível em: <ftp://ftp.ibge.gov.br/Acesso_a_internet_e_posse_celular/2011/PNAD_Inter_2011.pdf>. Acesso em: 25 set. 2016, p. 32.

² MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO. Instituto Brasileiro de Geografia e Estatística (IBGE). Pesquisa Nacional por Amostra de Domicílios (PNAD 2016): Acesso à internet e à televisão e posse de telefone móvel celular para uso pessoal, 2016. Disponível em: <http://biblioteca.ibge.gov.br/visualizacao/livros/liv95753.pdf>. Acesso em 9 abr. 2016, p. 44.

Nesse cenário, além de ser visualmente factível, está estatisticamente comprovado que as relações sociais atuais, quando não dependem, ao menos perpassam por algum meio virtual, que, em razão da sua intangibilidade, depende da disponibilização de dados pessoais para que os sujeitos se tornem minimamente identificáveis.

A respeito de dados pessoais, cumpre salientar o conceito formulado por Castro (2005, p. 70-71), segundo a qual:

Dado pessoal é o dado relacionado a um indivíduo identificado ou identificável, independentemente do suporte em que se encontra registrado (escrita, imagem, som ou vídeo). Entende-se por identificado o indivíduo que já é conhecido; e por identificável, a pessoa que pode ser conhecida diretamente pelo próprio possuidor de seus dados, ou indiretamente através de recursos e meios à disposição de terceiros.³

Diante desse panorama, tem-se, portanto, a sociedade da informação, que, ao ser considerada como um recorte da estrutura social, caracteriza-se, ao olhar de Vieira (2007, p. 156) como “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”.

Ascensão (2001, p. 46), por sua vez, ao escrever a respeito da sociedade da informação, explicou que essa nova conjuntura social tem por elemento básico e indispensável a gestão da informação e de dados pessoais, uma vez que tais fatores constituem a força motriz para um processo de comunicação integral.⁴

Ainda de acordo com Ascensão (2001, p. 70), a sociedade da informação se compõe dos seguintes elementos: objeto, que são os produtos de mídia e as bases

³ A fim de contextualizar, cumpre mencionar que o conceito formulado pela autora está baseado no artigo 2º, alínea ‘a’, da Diretiva 95/46 do Parlamento Europeu e do Conselho, segundo o qual dado pessoal “é qualquer informação relativa a uma pessoa singular identificada ou identificável (pessoa em causa); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social”. No Brasil, o conceito de dado pessoal está estabelecido no artigo 4º, inciso IV, da Lei n. 12.527/2011 – Lei do Acesso à Informação, segundo a qual “considera-se informação pessoal aquela relacionada à pessoa natural identificada ou identificável”.

⁴ Contudo, Ascensão (2001, p. 46) ressalva que: “Sociedade da informação não é um conceito técnico: é um *slogan*. Melhor sealaria até em sociedade da comunicação, uma vez que o que se pretende impulsionar é a comunicação e só num sentido muito lato se pode qualificar toda mensagem como informação”.

de dados eletrônicas;⁵ um veículo, que são as autoestradas da informação;⁶ e um resultado, que é a própria sociedade da informação, que se coloca como um fato incontroverso⁷.

Diante desse conceito, é importante mencionar que, embora as circunstâncias elementares à sociedade da informação remetam a uma condição social atual, tem-se, na verdade, que a sua formulação fora forjada muito antes disso, mais precisamente a partir da década de 80, quando Estados Unidos e Japão fortemente desenvolveram os seus tecnocentros (GERMAN, 2000, p. 16).

Em continuidade, no ano de 1993, o termo sociedade da informação foi oficialmente utilizado pela primeira vez, quando Jacques Delors, então presidente da Comissão Europeia, empregou-o para se referir ao uso da tecnologia como instrumento de catalisação da economia, dos serviços públicos e da qualidade de vida dos cidadãos (VIEIRA, 2007, p. 156).

A par desse contexto, não restam dúvidas que o uso da tecnologia e a gestão das informações, com o passar dos anos, além de terem se desenvolvido, ganharam relevante valor social e mercadológico, pois, em razão da sua pretensa utilização como elementos de fomento à economia e à atividade estatal, resta evidente que o controle de dados se tornou uma atividade de elevado valor e, conseqüentemente, de alto risco, o que implica, por consequência, na alteração e ressignificação dos valores básicos da ordenação social.

Além do mais, o incessante processo de informatização das relações pessoais, além de potencializar a coleta e armazenamento de dados, tem o condão de aproximar a oferta de produtos e serviços a potenciais consumidores, pois, ante a possibilidade de se traçar um perfil do usuário virtual, pode-se conceber suas preferências de consumo, o que obviamente denota as diversas implicações sociais e jurídicas dessa nova ordem social.

Nesse sentido, Tomé (2000, p.19-20) pondera que:

⁵ Segundo o autor (2001, p. 72), as bases de dados eletrônicas são pressuposto essencial para a sociedade da informação, uma vez que elas buscam reunir quase a totalidade da informação disponível e que seja objeto de procura, para colocá-las ao acesso de qualquer um.

⁶ Ao tratar das autoestradas da informação, Ascensão (2001, p. 84) conceitua-as como os meios de comunicação entre computadores, que se caracterizam pela grande capacidade, rapidez e fidedignidade.

⁷ Na dicção de Leonardi (2012, p. 71): “De fato, é preciso compreender que mais do mesmo pode representar algo completamente novo: grandes quantidades de informação sempre estiveram disponíveis de modo esparso, mas a possibilidade de análise e agregação de todos esses dados por qualquer pessoa, e não apenas por governos e por empresas, é algo inédito”.

Como punto de partida en el examen de tal fenómeno, debe destacarse el hecho de que el desarrollo y la universalización de las nuevas tecnologías de la información y las comunicaciones, si bien provocan una revolución técnica en el estado de la ciencia, no agotan ahí sus efectos. Su impacto es también cultural, económico, legal y social. (...) El carácter universal y más accesible que los últimos años han adquirido los recursos informáticos, unido al desarrollo de las nuevas tecnologías, ha propiciado el que la informatización de la sociedad, anunciada desde finales de los años setenta, se haya convertido en una realidad concreta en una nueva forma de organización social. Este fenómeno engendra una revolución que, a decir de algunos, tendrá una incidencia equivalente a la que tuvo la revolución industrial hace un siglo. Las nuevas tecnologías configuran la información como uno de los valores fundamentales de nuestra sociedad. Estamos caminando desde una forma de vida asentada en los bienes físicos hacia una centrada en el conocimiento y la información.⁸

Logo, nota-se que a informação, como matéria-prima deste novo recorte sociológico, torna-se uma condição determinante à segurança do Estado e um instrumento definidor de riqueza privada, pois, na medida em que permite o Estado conhecer os sujeitos que se utilizam de seus serviços e atravessam suas fronteiras, também confere ao gestor privado desses dados um poder de barganha extremamente relevante, uma vez que, ao titularizar essas informações, pode intensificar, perante a sociedade de consumo⁹, a aquisição de produtos e serviços mesmo que não conscientemente desejados.

Nessa direção, Castells (2000, p. 77) afirma que a sociedade se encontra amparada no Informacionalismo (ou capitalismo informacional), tendo em vista que o armazenamento e tratamento de informações se tornaram a base material da atividade econômica e da organização social.

⁸ Como ponto de partida ao exame de tal fenômeno, deve-se destacar que o desenvolvimento e a universalização das novas tecnologias da informação e das comunicações, se bem provocam uma revolução técnica no estado da ciência, aí não esgotam seus efeitos. Seu impacto também é cultural, econômico, legal e social. (...). O caráter universal e mais acessível que os recursos informáticos adquiriram nos últimos anos, unido ao desenvolvimento das novas tecnologias, tem propiciado que a informatização da sociedade, anunciada desde o final dos anos setenta, se converteu em uma realidade que se concretiza em uma nova forma de organização social. Este fenômeno engendra uma revolução que, nos dizeres de alguns, terá um impacto equivalente ao que teve a revolução industrial há um século. As novas tecnologias configuram a informação como um dos valores fundamentais da nossa sociedade. Estamos caminhando de uma forma de vida assentada nos bens físicos a uma centrada no conhecimento e na informação.

⁹ A fim de contextualizar sociedade de consumo, Bauman (2008, p. 37) comenta: “Aparentemente, o consumo é algo banal, até mesmo trivial. É uma atividade que fazemos todos os dias, por vezes de maneira festiva, ao organizar um encontro com os amigos, comemorar um evento importante ou para nos recompensar por uma realização particularmente importante – mas a maioria das vezes é de modo prosaico, rotineiro, sem muito planejamento antecipado nem reconsiderações”.

Diante desse contexto, não restam dúvidas que os dados pessoais disponibilizados nos mais diferentes meios tecnológicos, em especial a Internet, configuram-se como o alimento deste conceito de sociedade de informação.

Além do mais, pode-se dizer que essa transformação social, amparada no potencial valor da informação, incentivou e acelerou o desenvolvimento de diversos instrumentos político-econômicos e meios de interação social, uma vez que facilitou o acesso a conteúdos que, a depender da sua disposição física, jamais poderiam ser contatados.

Em contrapartida, a gestão desses dados como instrumentos da política e economia também pode se revelar como algo extremamente nocivo, uma vez que a agilidade, a interconexão e a eficiência dos sistemas eletrônicos podem tornar o sujeito, ainda que no âmbito de relações meramente privadas, absolutamente identificável¹⁰ e, por consequência, mais vulnerável.

Nesse viés, Silva e Silva (2013, p. 05-06) comentam que:

Sob o signo do desenvolvimento tecnológico acelerado, a cada dia são lançados novos aplicativos e criadas ferramentas e ambientes virtuais para encantar um público que não cessa de crescer. E, seduzidos pelas novas oportunidades de interconexão, os internautas (especialmente os brasileiros) revelam-se assíduos utilizadores de *sites* de redes sociais, *blogs* e *microblogs*, nos quais disponibilizam e divulgam voluntariamente suas informações pessoais, sem se preocupar com quem irá acessá-las ou para qual finalidade serão utilizadas [...]. Quando se trata de Internet, o tema ganha ainda mais interesse, tendo em vista a possibilidade de criação de perfis psicológicos que relevam os hábitos de consumo, os gostos e preferências do indivíduo e, uma vez formado o perfil, posteriormente esse consumidor passa a ser alvo de publicidades indesejadas, e-mails que oferecem serviços, produtos e uma série de outras promoções que parecem elaboradas e direcionadas especialmente a ele, tudo articulado com base nos dados antes recolhidos. Percebe-se, pois, que as novas tecnologias informacionais, especialmente a Internet, convertem a informação em uma riqueza fundamental da sociedade, o que acentua a necessidade de sua proteção.

¹⁰ A esse respeito, Vieira (2007, p. 225-226) relata que: “na sociedade da informação, as pessoas cada vez mais se encontram controladas por potentes *softwares* de cruzamento e busca de informações. Desde o nascimento, o indivíduo já tem inseridos os respectivos dados pessoais em arquivos informatizados da Secretaria de Registro Civil. Ao longo dos anos, passa a integrar também os arquivos da Secretaria de Segurança Pública, do Conselho Nacional de Trânsito, da Receita Federal, dos conselhos profissionais e outros. Isto sem mencionar os registros de estabelecimentos médicos, de instituições financeiras, de estabelecimentos de ensino, associações, lojas, bibliotecas e de tantos outros estabelecimentos. Essas informações, uma vez coletadas, são armazenadas em bancos de dados ligados em rede, o que permite a interconexão dos arquivos e a definição do perfil dos seus titulares, medida que se consuma em alta velocidade, com baixo custo e com pequena margem de erro. Neste caso, até os dados mais irrelevantes passam a ter importância”.

Para mais, impende salientar que a sociedade da informação, como substrato ao fomento do comércio eletrônico, enseja um desequilíbrio ainda maior entre o fornecedor e o consumidor, uma vez que este, além de ter que repassar ao meio eletrônico informações relevantes à sua privacidade, perde o contato imediato com o produto ou serviço que pretende adquirir, o que, invariavelmente, pode refletir na sua decisão.

Logo, pode-se sustentar que esse novo cenário, capitaneado pela sociedade da informação, impôs ao usuário digital uma condição de vulnerabilidade informacional, pois, ao passo que o internauta recebe apenas as informações necessárias ao cumprimento de seu intento, o órgão gestor desses dados passa a concentrar um infindável número de informações que, quando mal utilizadas, podem ser extremamente prejudiciais à pessoa a quem se referem.¹¹

Ao tratar desse tipo de vulnerabilidade, Limberger e Moraes (2015, p. 262) mencionam que:

Sobre o assunto, destaca-se a caracterização da vulnerabilidade técnica, a qual se configura por uma série de motivos, sendo os principais: a falta de informação, informações prestadas incorretamente e, até mesmo, o excesso de informações desnecessárias, esta última, muitas vezes, tendo o condão de impedir que o consumidor se aperceba daquelas que realmente interessam. Enfatiza-se, ainda, a dificuldade de o consumidor possuir conhecimentos específicos acerca das propriedades, dos malefícios e das consequências em geral da utilização ou contato com os modernos produtos ou serviços.

Na mesma direção, Ascensão (2001, p. 78-79) argumenta que, à medida que a abrangência da sociedade da informação aumenta, a desproteção do consumidor se potencializa em proporção geométrica, sobretudo ao se considerar a internacionalização do sistema, o que retira cada vez mais do usuário o controle sobre a informação disponibilizada.

Não bastasse essa hiperfragilização do cidadão frente aos meios tecnológicos, o contexto da sociedade da informação, ao se pautar pelo valor social e econômico dos dados, torna-se capaz de transformar a pessoa humana em mercadoria (BAUMAN, 2008), pois, ao considerar que essas informações podem

¹¹ Vieira (2007, p. 227), ressalva que: “Mesmo que as informações sejam corretas, ainda assim haverá dano, caso os dados sejam divulgados ou acessados indevidamente por terceiros mal-intencionados. É recomendável, portanto, que o titular seja informado de que seus dados estão sendo coletados e armazenados em banco de dados, em relação aos quais se permitirá esse mesmo titular acesso, para conhecimento, correção e atualização”.

definir o perfil do usuário que a disponibilizou, o seu manejo, por uma perspectiva bastante utilitarista, interessa a muitos fornecedores, sejam eles virtuais, ou não.

Sob essa perspectiva, Bioni (2014, p. 297) assevera que:

Os dados pessoais estão, efetivamente, monetizados, consistindo na moeda de troca – o *tradeoff* – da maioria dos modelos de negócio na internet, os quais são rentabilizados pela publicidade direcionada que se vale, justamente, das informações pessoais dos usuários para lhes direcionarem anúncios publicitários. É, portanto, o caráter econômico das informações pessoais dos usuários que soluciona a equação econômica dos bens de consumo em médio a sociedade da informação, remunerando-os indiretamente.

Diante de todas essas colocações, não restam dúvidas que a gestão de dados pessoais, no âmbito da sociedade da informação, está em incessante embate com alguns direitos fundamentais, especialmente a privacidade, o sigilo das comunicações e dos dados, e a até mesmo a liberdade, os quais estão previstos no artigo 5º da Constituição Federal.

No que se refere à liberdade, destaca-se que, na medida em que informações pessoais são acumuladas, especialmente pelo Estado, tem-se a construção de uma espécie de panóptico eletrônico, uma vez que, em nome da segurança, a utilização desses arquivos ganha irremediável e efetiva função de vigilância,¹² o que indubitavelmente coloca o sujeito numa condição de passividade absoluta e, por consequência, prejudica o sigilo necessário à expressão de algumas atividades e/ou posicionamentos, o que também interfere no direito à privacidade.

A partir desse prisma, Castells (2003, p. 148-149) esclarece que:

O aspecto mais atemorizante é, de fato, a ausência de regras explícitas de comportamento, de previsibilidade das consequências de nosso comportamento exposto, segundo os contextos de interpretação, e de acordo com critérios usados para julgar nosso comportamento por uma variedade de atores atrás da tela de nossa casa de vidro. Não é o Big Brother, mas uma multidão de irmãszinhas agências de vigilância e processamento de informações que registram nosso comportamento para

¹² A esse respeito, Vieira (2007, p. 174) expõe que: “Assim, a vigilância, antes exercida pela família e pela Igreja, aos poucos é transferida para o Estado diante da maior complexidade da sociedade e da necessidade de gerenciamento das informações. [...]. O método passou a ser utilizado pelos governos para facilitar o desempenho de diversas atividades tais como arrecadação tributária; criação de um arquivo central com a classificação dos cidadãos de acordo com suas atividades produtivas, patrimônio e outros dados relevantes; manutenção da lei e da ordem pública por meio da vigilância de grupos de oposição; elaboração de estatísticas; dentre outras. A intromissão do Estado na privacidade dos cidadãos por meio da coleta de informações pessoais e uso de recursos tecnológicos configura-se, nesse contexto, como um mecanismo de poder necessário para benefício da população”.

sempre, enquanto banco de dados nos rodeiam ao longo da nossa vida – a começar, dentro em breve, com nosso DNA e características (nossa retina, nosso datilograma, na forma de marcas digitalizadas). Nas condições vigentes nos Estados autoritários, essa vigilância pode afetar diretamente nossas vidas (essa é de fato a situação da maioria esmagadora da humanidade). Mas mesmo em sociedades democráticas, em que os direitos civis são respeitados, a transparência de nossas vidas moldará decisivamente as nossas atitudes. Ninguém jamais foi capaz de viver numa sociedade transparente. Se esse sistema de vigilância e controle da Internet se desenvolver plenamente, não poderemos fazer o que nos agrada. Talvez não tenhamos nenhuma liberdade e nenhum lugar onde nos esconder.

Sob uma perspectiva de relações unicamente privadas e em referência apenas à privacidade e ao sigilo de dados, denota-se que a utilização da internet e das demais tecnologias, ao terem por praxe a gravação, ainda que indireta, dos registros de dados do usuário, permite que seja feita a representação de ao menos uma parcela da individualidade do sujeito, o que, ao poder ser manejado de forma velada, coloca em risco os direitos fundamentais do cidadão (VIEIRA, 2007, p. 176).

À vista disso, tem-se o fato de que a sociedade da informação, para continuar a se perpetuar, necessita que seja feita uma verdadeira biografia dos cidadãos que permita o fácil e rápido conhecimento do interlocutor (BIONI, 2014, p. 298), o que, de certa forma, remete à sua autossuficiência, já que o crescimento - ou ao menos a manutenção - do volume da coleta de dados depende da criação e disponibilização de novos mecanismos tecnológicos para os mais variados fins.

Todavia, a gestão desses dados coloca os direitos fundamentais à privacidade, ao sigilo dos dados, às comunicações e à liberdade em uma situação perante a qual merecem ser resignificados, haja vista que a sua tutela, nos moldes clássicos, mostra-se insuficiente a esse novo contorno sociológico.

Logo, ao se ter nos dados pessoais uma projeção dos direitos fundamentais à personalidade e, tendo por base a amplitude da sociedade da informação e o alto valor subjetivo e objetivo do seu elemento básico, faz-se necessário e absolutamente relevante compreender com quais fundamentos pode se dar uma proteção jurídica efetiva a essas informações, afinal, ante ao ínsito potencial danoso da evolução tecnológica em face das sociedades atuais, torna-se imprescindível conhecer mecanismos para anular, ou ao menos amenizar esses impactos (EFING, 2002, p, 43), sob pena de se colocar o cidadão num estado de vulnerabilidade inexorável.

3 A PROTEÇÃO DOS DADOS PESSOAIS NA LEGISLAÇÃO BRASILEIRA

Ao se analisar a proteção dos dados pessoais com base na legislação pátria, deve-se destacar, de antemão, que esse exame necessita de uma compreensão sistêmica do ordenamento jurídico, pois, do contrário, isto é, ao se tomar um diploma legislativo de forma isolada, estar-se-ia a ignorar toda a estrutura do conjunto de normas nacional, e o objeto dessa pesquisa, por consequência, seria reduzido a elementos que, sozinhos, não se mostrariam juridicamente efetivos, já que a proteção de dados no contexto da sociedade da informação ficaria restrita apenas a alguns tipos de relações privadas, especialmente as de consumo, que possuem regramento específico e indeclinável, haja vista que sua regulação se dá com base em normas de ordem pública e interesse social.

Entretanto, intenta-se, com o presente trabalho, conferir uma visão mais ampla à proteção dos dados pessoais, motivo pelo qual, inclusive, inicia-se a análise legislativa pela Constituição Federal, uma vez que esse corpo normativo, por ser central ao ordenamento jurídico, serve de fundamento aos demais regulamentos.¹³

Sob a perspectiva constitucional, é possível vislumbrar que a proteção aos dados pessoais possui fundamento em diversos dispositivos, com especial atenção ao artigo 5º, incisos X e XII, que positivam os direitos fundamentais à privacidade e ao sigilo de dados e das comunicações; e aos artigos 5º, inciso XXXII e 170, inciso V, que preveem a defesa do consumidor como um dever do Estado e como um dos princípios da ordem econômica brasileira.

Além desses dispositivos isoladamente considerados, a proteção constitucional aos dados pessoais também se perfaz em sua análise sistêmica, pois, ao se coadunar os dispositivos acima mencionados, alcança-se o princípio da autodeterminação informativa, que se mostra como um elemento essencial à

¹³ À vista disso, ressalta-se o sentido jurídico da Constituição, delineado por Hans Kelsen, sobre o qual Silva (2013, p. 41), ao escrever a respeito, declarou: “no sentido jurídico, constituição é, então, considerada *norma pura*, puro *dever-ser*, sem qualquer pretensão a fundamentação sociológica, política ou filosófica. A concepção de Kelsen toma a palavra constituição em dois sentidos: no *lógico-jurídico* e no *jurídico-positivo*; de acordo com o primeiro, constituição significa *norma fundamental hipotética*, cuja função é servir de fundamento lógico transcendental da validade da constituição *jurídico-positiva* que equivale à norma positiva suprema, conjunto de normas que regula a criação de outras normas, lei nacional no seu mais alto grau. No mesmo sentido, Mendes e Branco (2012, p. 74) argumentam que: “As normas constitucionais, situadas no topo da pirâmide jurídica, constituem o fundamento de validade de todas as outras normas inferiores e, até certo ponto, determinam ou orientam o conteúdo material dessas últimas”.

proteção do cidadão ante a voracidade e agilidade do fluxo de dados na sociedade da informação.

No que concerne ao plano infraconstitucional, diversos são os diplomas legislativos com disposições aplicáveis à proteção dos dados pessoais na internet.

Nessa esteira, merecem destaque o Código de Defesa do Consumidor, o qual, tanto por meio das suas regras quanto por seus princípios, instrumentaliza usuário digital com diversas garantias capazes de frear o uso de indevido dos dados pessoais, especialmente no âmbito do comércio eletrônico; o Decreto n. 7.962/2013, que, ao regulamentar a contratação eletrônica, reforçou as disposições do Código de Defesa do Consumidor e esclareceu que o fornecedor que se vale do meio digital deve se esforçar ainda mais para o perfeito adimplemento do contrato firmado; e a Lei n. 12.965/2014, popularmente conhecida como Marco Civil da Internet, que estabeleceu os princípios, garantias, direitos e deveres para o uso da internet no Brasil.

Tendo por base esse contexto, passa-se a análise constitucional da proteção dos dados pessoais na internet.

3.1 A PROTEÇÃO CONSTITUCIONAL DOS DADOS PESSOAIS

Ao se começar a falar a respeito da proteção de dados pessoais, é comum que, em um rápido raciocínio, venha a mente os direitos fundamentais à privacidade, intimidade e sigilo da dados e comunicações.

Aliás, nem poderia ser diferente, afinal, a primeira esfera do ser humano a ser violada quando da utilização inadequada dos registros de dados é, indubitavelmente, a privacidade,¹⁴ aqui considerada em seu sentido mais amplo¹⁵.

¹⁴ Por esse prisma, Efig (2002, p. 59) comenta que: “Atingem a intimidade do ser humano ao perpetuar sem sua aprovação, na maioria das vezes sem seu conhecimento, informações que não pretendia ver na *boca do povo*, traíndo sua confiança, e proporcionando agruras fundadas na deslealdade, atingindo o âmago do indivíduo, Além disso, ao investigar e divulgar os dados pessoais, os repositórios de consumo infringem o direito fundamental à vida privada, visto que os dados constantes dizem respeito à vida pessoal do cidadão, que na maioria das vezes sequer tem conhecimento desta publicação. Mais ainda, tanto a honra objetiva quanto a subjetiva são abalroadas pela prática dos arquivos de consumo, quando fazem desmoronar sentimentos interiores e exteriores a respeito do indivíduo”.

¹⁵ Em relação à abrangência do conceito de privacidade, Mendes e Branco (2012, p. 318) ressaltam que: “Embora a jurisprudência e vários autores não distingam, ordinariamente, entre ambas as postulações – de privacidade e de intimidade -, há os que dizem que o direito à intimidade faria parte

A par dessa colocação, cumpre destacar que o direito à privacidade ordinariamente remete o indivíduo a sua esfera privada, a um reduto em que não se pode haver interferência de fora, a um local em que as amarras do cotidiano são ignoradas.

Nessa direção, Mendes e Branco (2012, p. 318-19) dizem que:

A reclusão periódica à vida privada é uma necessidade de todo homem para a sua própria saúde mental. Além disso, sem privacidade, não há condições propícias para o desenvolvimento livre da personalidade. Estar submetido ao constante crivo da observação alheia dificulta o enfrentamento de novos desafios. A exposição diuturna dos nossos erros, dificuldades e fracassos à crítica e à curiosidade permanente de terceiros, e ao ridículo público mesmo inibiria toda tentativa de autossuperação. Sem a tranquilidade emocional que se pode auferir da privacidade, não há muito menos como o indivíduo se auto avaliar, medir perspectivas e traçar metas.

Nesse cenário, nota-se que a privacidade se caracteriza como um direito fundamental negativo, isto é, como um direito de defesa à intervenção de terceiros, sejam eles entes privados – ao se considerar sua dimensão horizontal¹⁶, ou mesmo o Estado, que, originariamente, é o principal destinatário das limitações impostas pelos direitos fundamentais de primeira geração,¹⁷ pois, tendo por base os traços

do direito à privacidade, que seria mais amplo. O direito à privacidade teria por objeto os comportamentos e acontecimentos atinentes aos relacionamentos pessoais e geral, às relações comerciais e profissionais que o indivíduo não deseja que se espalhem ao conhecimento público. O objeto do direito à intimidade seriam as conversações e episódios ainda mais íntimos, envolvendo as relações familiares e amizades mais próximas”. Ao discorrerem sobre o direito fundamental ao sigilo de dados e das comunicações, os autores (2012, p. 333-334) ponderam que: “O sigilo das comunicações é não só um corolário da garantia da livre expressão de pensamento; exprime também aspecto tradicional do direito à privacidade e à intimidade. A quebra da confidencialidade da comunicação significa frustrar o direito do emissor de escolher o destinatário do conteúdo da sua comunicação”.

¹⁶ Segundo Mendes e Branco (2012, p. 200-201): “A percepção clara da força vinculante e da eficácia imediata dos direitos fundamentais e da sua posição no topo da hierarquia das normas jurídicas reforçou a ideia de que os princípios que informam os direitos fundamentais não poderiam deixar de ter aplicação também no setor do direito privado. Ganhou alento a percepção de que os direitos fundamentais possuem uma feição objetiva, que não somente obriga o Estado a respeitar os direitos fundamentais, mas que também o força a fazê-los respeitados pelos próprios indivíduos, nas ruas relações entre si. Ao se desvendar o aspecto objetivo dos direitos fundamentais, abriu-se à inteligência predominante à noção de que esses direitos, na verdade, exprimem os valores básicos da ordem jurídica e social, que devem ser prestigiados em todos os setores da vida civil, que de devem ser preservados e promovidos pelo Estado como princípios estruturantes da sociedade. O discurso majoritário adere, então, ao postulado de que ‘as normas sobre direitos fundamentais apresentam, ínsitas a elas mesmas, um comando de proteção, que obriga o Estado a impedir que tais direitos sejam vulnerados também nas relações privadas’.

¹⁷ Na dicção de Mendes e Branco (2012, p. 155), a primeira geração dos direitos fundamentais “abrange os direitos referidos nas Revoluções americana e francesa. São os primeiros a ser positivados, daí serem ditos de primeira geração. Pretendia-se, sobretudo, fixar uma esfera de autonomia pessoa refratária à expansão do Poder. Daí esses direitos traduzirem-se em postulados de abstenção dos governantes, criando obrigações de não fazer, de não intervir sobre aspectos da vida

acima delineados, entende-se que o exercício do direito à privacidade não depende de uma atitude própria, mas sim dos outros.

À guisa dessa conclusão, Mendes e Branco (2012, p. 321) asseveram que o direito à privacidade “conduz à pretensão do indivíduo de não ser foco da observação por terceiros, de não ter os seus assuntos, informações pessoais e características particulares expostas a terceiros ou ao público em geral”.

Todavia, ante o contexto da sociedade da informação, o direito fundamental à privacidade não pode ser reduzido a sua dimensão negativa. É dizer: ao se disponibilizar os dados pessoais em meio eletrônico, o utente não pode ficar à mercê da discricionariedade do gestor do banco de dados, ainda que os princípios da boa-fé objetiva e confiança infraconstitucionalmente previstos assim o garantam, sobretudo ao se considerar a intangibilidade, a complexidade e a agilidade do meio, que, em questão de minutos, é capaz de conferir múltiplas destinações e funções à informação voluntariamente disponibilizada.¹⁸

Privacidade no âmbito da sociedade da informação exige mais, isto é: requer uma prestação positiva e por isso deve ser ressignificada.

Nessa direção, destaca-se, inicialmente, as lições de Rodotà, segundo o qual o direito à privacidade não mais se restringe ao eixo “pessoa-informação-segredo”, mas se perfaz sobre o conceito de “pessoa-informação-circulação-controle”, o que, por consequência, traz ao conceito de privacidade duas novas exigências, quais sejam: os deveres do gestor do banco de dados em dar conhecimento da situação da informação a quem a disponibilizou; e de possibilitar o exercício de um controle ativo por parte do seu titular.

A esse respeito, Leonardi (2012, p. 67-68) explica que:

O direito à privacidade deve ser compreendido como um direito de controle sobre informações e dados pessoais. Para essa corrente, a privacidade é a reivindicação de indivíduos, grupos ou instituições de determinar por si próprios, quando, como e em que extensão informações a seu respeito são comunicadas a terceiros. O atributo básico do direito à privacidade seria,

pessoal de cada indivíduo. São considerados indispensáveis a todos os homens, ostentando, pois, pretensão universalista”.

¹⁸ Nesse panorama, Silva (2013, p. 211-212) argumenta que: “O intenso desenvolvimento de complexa rede de fichários eletrônicos, especialmente sobre dados pessoais, constitui poderosa ameaça à privacidade das pessoas. O amplo sistema de informações computadorizadas gera um processo de esquadramento das pessoas, que ficam sua individualidade inteiramente devassada. O perigo é tão maior quanto mais a utilização da informática facilita a interconexão de fichários com a possibilidade de formar grandes bancos de dados que desvendem a vida dos indivíduos, sem sua autorização e até mesmo sem seu conhecimento”.

portanto, a capacidade de o indivíduo controlar a circulação de informações a seu respeito. Em oposição às correntes, a privacidade não é a simples ausência de conhecimento alheio sobre fatos da vida privada do indivíduo, mas sim o controle exercido sobre essas informações e esses dados pessoais.

Em complemento a essa colocação, Efing (2002, p. 58), ao destacar a indeclinabilidade do direito à privacidade, ressalta que o conhecimento, a coleta o destino e a finalidade para qual os dados foram disponibilizados devem, logicamente, serem respeitados, afinal, tendo em vista que a Constituição Federal categorizou a privacidade como um direito fundamental, é inconteste o seu caráter de direito público subjetivo, o que, indubitavelmente, passa as mãos do seu titular a prerrogativa de exigir o seu manejo sob as condições de seu interesse.¹⁹

Diante dessa nova contextualização, verifica-se que o direito à privacidade, além de ser uma defesa passiva às interferências indevidas ao âmbito privado, caracteriza-se como um poder de resistência às intromissões indesejadas, pois, ao se atribuir ao gestor do banco de dados o dever de dar conhecimento, ao titular do dado pessoal, do estado em que se encontra sua informação, e ao se instrumentalizar o sujeito com elementos que permitam um controle efetivo sobre o fluxo de dados a seu respeito, cria-se um dever/direito à transparência, o que, irremediavelmente, é um poderoso instrumento de vigilância e correção de eventuais equívocos ou desvios.

Em razão dessa nova dimensão da privacidade, chega-se a afirmar, inclusive, que esse direito fundamental passou a ter uma significação social, embora comumente o seu tratamento ocorra sob o título de garantia individual, sob a justificativa de que o seu exercício ativo tem a capacidade de assegurar o equilíbrio da estrutura social, haja vista a sua capacidade em conter abusos ocasionais.

Por essa perspectiva, Rodotà (1995, p. 27), pondera que:

A evocação da privacidade supera o tradicional quadro individualista e se dilata em uma dimensão coletiva, a partir do momento em que deixa de considerar o interesse do indivíduo enquanto tal, para reconhecê-lo como membro de um determinado grupo social.

¹⁹ Ainda segundo o autor (p.48): “Os direitos fundamentais impõem tutela negativa e positiva. A função negativa se revela como sua função originária, consistente em proibir o Estado de interferir nesta esfera autônoma de atuação de cada cidadão individualmente considerado. A positiva, por sua vez, constitui a imposição de ação comissiva do Estado para a garantia da efetivação destes direitos fundamentais, integrando em suas ações o cidadão”.

Ao mesmo tom, Leonardi (2012, p. 122) assevera que:

Não se deve entender a tutela da privacidade como a proteção exclusiva de um indivíduo, mas sim como uma proteção necessária para a manutenção da estrutura social. A privacidade não é valiosa apenas para a vida privada de cada indivíduo, mas também para a vida pública e comunitária. Como destaca Gustavo Tepedino, o direito à privacidade consiste em uma tutela indispensável ao exercício da cidadania. Atribuir valor social à privacidade não significa dizer que os danos morais sofridos pelos indivíduos sejam irrelevantes. Apenas se exige a constatação de que, além de um interesse individual, há benefícios sociais que justificam sua tutela, ainda que a conduta de indivíduos no caso concreto possa ser moralmente reprovável.

À vista disso, observa-se que essa dimensão ativa do direito fundamental à privacidade, além de ser necessária para dar conta das situações criadas pela sociedade da informação, mostra-se socialmente benéfica, uma vez que possibilita aos indivíduos a efetivação de um controle eminentemente coletivo, ainda que os sujeitos não o façam em unidade de desígnios e mediante divisão de tarefas.

Para mais, pode-se afirmar que essa ressignificação do direito fundamental à privacidade é materialmente suficiente para dar azo à aplicabilidade do princípio da autodeterminação informativa, o qual, apesar de não estar expressamente previsto no texto constitucional, nele encontra seu fundamento de validade.

Ao escrever sobre a autodeterminação informativa, Bioni (2014, p. 298) traz o seguinte conceito:

A autodeterminação informacional consiste, em suma, na perspectiva de que o indivíduo deve controlar (autodeterminar) os seus dados pessoais (informações pessoais: autodeterminação informacional), exigindo-se, por isso, o consentimento do titular das informações pessoais para que elas sejam coletadas, processadas e compartilhadas.

Eiras (1992, p. 78), por seu turno, chega a dizer que a autodeterminação informativa se caracteriza como um superconceito, já que o seu conteúdo normativo se desdobra em diversos aspectos.

Nesse sentido, o autor comenta que:

O direito à autodeterminação informacional é um superconceito que se desdobra em vários outros, a saber: a) o direito de acesso aos ficheiros, que confere ao cidadão o direito a tomar conhecimento de quaisquer registos por forma compreensível, em linguagem clara, isenta de codificação e em prazo razoável; b) o direito de, em certos casos, se opor ao registo de dados e a que essa oposição fique registrada; c) o direito a ser informado acerca do motivo por que lhe é recusado o direito de acesso; d) o direito de ser esclarecido acerca do objetivo que determinou a inserção dos dados no

ficheiro; e) o direito de contestação, que engloba a faculdade de exigir a rectificação dos dados armazenados inexactos, a faculdade de exigir a correção dos dados que estejam desactualizados, a faculdade de exigir a eliminação de dados constantes dos registos contra regras ou princípios constitucionais, a faculdade de exigir o cancelamento de dados decorrido determinado período (direito ao esquecimento).

Diante desse conceito, verifica-se que a autodeterminação informativa se perfaz justamente na ressignificação do conceito de privacidade, é dizer: o fundamento desse princípio reside, basicamente, na dimensão ativa desse direito fundamental, já que o seu conteúdo consiste na passagem, ao titular dos dados, da prerrogativa de definir os destinos das informações que coloca à disposição de terceiros.

À vista disso, destaca-se, com base nos apontamentos de Vieira (2007, p. 268-269) que esse princípio surgiu como uma construção jurisprudencial da Corte Constitucional Alemã, que, ao se manifestar a respeito da Lei do Censo de 1983, julgou-a inconstitucional no que se referia à obrigatoriedade, por parte dos cidadãos alemães, de responderem um questionário com informações pessoais, para que esses dados pudessem ser confrontados com outros registos já existentes em repartições públicas federais, estaduais e municipais, o que esvaziaria qualquer possibilidade de controle por parte dos indivíduos. Nesse contexto, o Tribunal Constitucional alemão reconheceu que os dados pessoais guardam inequívoca relação com os direitos da personalidade, razão pela qual julgou nulo o dispositivo que possibilitava o repasse autônomo de informações pessoais e, com isso, reconheceu o princípio da autodeterminação informacional (*Recht auf Informationelle Selbstbestimmung*).

No Brasil, não existem nos Tribunais superiores registos precisos gravados sob a rubrica da autodeterminação informativa. Em contrapartida, alguns Tribunais locais, especialmente os do Rio de Janeiro e Rio Grande do Sul, já recorreram a esse conceito para orientar suas decisões, notadamente quando são instados a se manifestar a respeito da inscrição de consumidores em cadastros de crédito²⁰.

Dentre esses julgados, sobressalta-se um voto proferido pela Desembargadora Maria Cláudia Mércio Cachapuz, do Tribunal de Justiça do Rio Grande do Sul, no julgamento da apelação cível n. 70061072203, em que se discutia

²⁰ Apelação Cível n. 70060085438, do Tribunal de Justiça do Rio Grande do Sul; Apelação Cível n. 0193382-67.2011.8.19.0001, do Tribunal de Justiça do Rio de Janeiro, por exemplo.

se os arquivos de crédito utilizados para a avaliação do histórico financeiro do consumidor eram compatíveis, ou não, com o direito brasileiro.

Na referida decisão, a Excelentíssima Magistrada, ao abordar o tema da autodeterminação informativa, demonstrou-o como fonte de novos direitos/obrigações, quais sejam: o dever do gestor do banco de dados em disponibilizar o acesso e conhecimento dos registros que maneja e o direito do cidadão em ativamente controlar a informação que dispôs em favor de terceiro, o que se mostra absolutamente consentâneo à abordagem trazida nesse trabalho.

Nessa direção, destaca-se o seguinte trecho do voto da Desembargadora (2015):

Como a ideia de autodeterminação informativa apropria-se de conceitos relacionados tanto a um espaço de interferência marcante do direito de liberdade (esfera privada) como de interferência mais acentuada do direito de igualdade (esfera pública), identifica-se também num direito de acesso a dados informativos a possibilidade de o indivíduo ter acesso a informações que lhe sejam justificadamente importantes ou de revelação essencial. Abstratamente, a hipótese responde ao conceito de autodeterminação informativa como trabalhado pelo Tribunal Constitucional Federal da Alemanha, pois exige a reciprocidade de conduta a quem se dispõe à liberação dos dados e a quem pretende obter determinado acesso. Ou seja, permite-se, pelo exercício da ponderação, a partir da análise de situações concretas envolvendo direitos fundamentais, que dados nominativos sejam tornados públicos quando suficientemente evidenciada a sua relevância ao interessado.

Nesse cenário, nota-se que o princípio da autodeterminação informativa, implicitamente previsto na Constituição Federal, não consiste apenas em mais um instrumento de segurança passiva dos dados pessoais, mas também se mostra como uma garantia da liberdade em se dispor das próprias informações exclusivamente com base na medida da sua consciência (CASTRO, 2011).

Para mais, tendo em vista que esse princípio exige um exercício de reciprocidade entre os bancos de dados e os titulares da informação, faz-se necessário, por consequência, o exercício de um dever jurídico de cooperação, o que retoma a dimensão social da privacidade acima delineada e contribui para a ultimação de um dos objetivos da República Federativa do Brasil, que é a construção de uma sociedade livre, justa e solidária.

A par dessas colocações, é possível afirmar que a proteção dos dados pessoais no contexto da sociedade da informação encontra um largo embasamento na Constituição Federal, pois, além desse copo normativo garantir aos cidadãos

uma defesa passiva, mediante a qual se atribui ao terceiro um dever jurídico de não agir, constata-se que a reinterpretação dessas normas, sem perder de vista a compatibilidade com a coerência sistêmica do texto, instrumentaliza o sujeito com a possibilidade de atuar comissivamente, ou seja, é direito do cidadão acompanhar de perto o tratamento que estão a dar às suas informações pessoais, haja vista que esses dados consistem em uma projeção real da sua personalidade.

No que se refere às normas previstas no artigo 5º, inciso XXXII, e artigo 170, inciso V, da Constituição Federal, que estipulam a defesa do consumidor como um dever do Estado e como um dos princípios da ordem econômica nacional, pode-se afirmar que nesses dispositivos reside o primeiro fundamento da vulnerabilidade do cidadão-consumidor, afinal, ao se reconhecer essas diretrizes como um direito fundamental, torna-se clara a necessidade de proteger a fragilidade desses sujeitos perante a voracidade da livre iniciativa e da economia de um país, agora potencializados no âmbito da sociedade da informação.

Além do mais, esses dispositivos constitucionais, por se caracterizarem como um direito público subjetivo, permitem que se exija do Estado uma postura ativa, isto é, autoriza que a Administração Pública se valha da imperatividade e autoexecutoriedade dos seus meios para que os direitos do cidadão-consumidor, em qualquer lugar e tempo, inclusive no meio eletrônico, sejam efetivamente respeitados.

Para mais, ao se retomar o conceito de eficácia horizontal dos direitos fundamentais, a defesa do consumidor também se coloca como um dever jurídico social dos entes privados, que, a despeito da livre iniciativa, devem condicionar suas atividades às balizas constitucionais e legais vigentes²¹, o que implica, por

²¹ Segundo Marques (2013, p. 34): “[...], como direito fundamental é um direito subjetivo (direito do sujeito, direito subjetivo público, geral, do cidadão), que pode e deve ser reclamado e efetivado por este sujeito de direitos constitucionalmente assegurados, o consumidor; seja contra o Estado (é a chamada eficácia vertical dos direitos fundamentais, eficácia entre o Estado e o consumidor dos direitos fundamentais) ou nas relações privadas (é a chamada eficácia horizontal dos direitos fundamentais, entre dois sujeitos do direito privado, por exemplo, efeito dos direitos fundamentais entre um consumidor e um banco [...]). Em outras palavras, o direito fundamental deve ser respeitado, respeitado de acordo e em conformidade com a lei infraconstitucional (eficácia indireta, pois através da norma infraconstitucional, dos direitos fundamentais, como o CDC) e as exigências da dignidade da pessoa humana (eficácia direta dos direitos fundamentais nas relações privadas) ”.

consequência, na sua colaboração para com as dimensões negativa e positiva do direito fundamental à privacidade.²²

Juntamente a isso, destaca-se que o tratamento da defesa do consumidor como um direito fundamental serve de aparato lógico-jurídico para toda a proteção infraconstitucional especializada, com especial atenção ao Código de Defesa do Consumidor, pois, é dessa garantia constitucional que a legislação densifica diversas regras que reforçam a proteção dos dados pessoais em meio eletrônico²³.

3.2 – A PROTEÇÃO INFRACONSTITUCIONAL AOS DADOS PESSOAIS

Ao se começar a falar sobre a proteção infraconstitucional aos dados pessoais no contexto da sociedade da informação, destaca-se, inicialmente, as regras e princípios previstos no Código de Defesa do Consumidor, pois, além desse corpo normativo disponibilizar aos cidadãos diversas ferramentas jurídicas de proteção - as quais, a propósito, são indeclináveis, já que possuem natureza de ordem pública -, destaca-se que grande parte do volume de dados pessoais que tramitam em âmbito eletrônico decorrem da prática do *e-commerce*, pois, ao que consta de pesquisa do E-bit (2016, p. 16), cerca de 39,1 milhões de consumidores efetuaram ao menos uma compra *online* em 2015, o que representou uma movimentação financeira de aproximadamente R\$ 41,3 bilhões.

À vista desse contexto, merecem destaque os direitos básicos do consumidor à segurança e à informação e o princípio da boa-fé objetiva, os quais, em conjunto, tutelam o consumidor em todos os momentos e aspectos da relação jurídica de consumo a ser firmada, dentre as quais, inclusive, estão as fases pré e pós-contratual.

No que concerne ao direito básico à segurança, previsto nos artigos 4º, incisos II e V, e 6º, inciso I, do Código de Defesa do Consumidor, a sua

²² Marques (2013, p.37-38) também pondera que: “Efetivamente, no Brasil de hoje, a proteção do consumidor é um valor constitucional fundamental (*Wertsystem*), é um direito fundamental e é um princípio da ordem econômica da Constituição Federal (art. 170, V), princípio limitador da autonomia da vontade dos fortes em relação aos fracos ou vulneráveis (*debilis*), construindo um novo direito privado mais consciente de sua função social”.

²³ Afinal, de acordo com Marques (2013, p. 36): “A Constituição Federal de 1988 serve, assim, de centro valorativo, centro sistemático-institucional e normativo também do direito privado (*força normativa da Constituição*), um novo direito privado brasileiro (*garantido e moldado pela ordem pública constitucional, limitado e consubstanciado pelos direitos fundamentais aí recebidos*) [...]”.

conceituação pode se dar de maneira simples. É dizer: o direito básico à segurança consiste na prerrogativa do consumidor em ser acautelado dos riscos inerentes ao objeto e às relações de consumo.

Na dicção de Marques (2013, p. 71), esse direito básico “impõe a todos os fornecedores um dever de qualidade dos produtos e serviços que presta e assegura a todos os consumidores [...] um direito de proteção, fruto do princípio da confiança e segurança (art. 4º, V, do CDC)”.

Nesse cenário, verifica-se que a leitura do direito básico à segurança deve se dar à luz da teoria da qualidade/adequação, já que nenhum produto e tampouco o meio pelo qual se formaliza a relação de consumo podem colocar o consumidor em situação de risco, a não ser aqueles que lhes são inerentes e, portanto, inafastáveis a determinado objeto ou condição.

Segundo Benjamin (2013, p, 148), “a teoria da qualidade forma-se com os olhos voltados para o instituto da responsabilidade do fornecedor: civil, administrativa e penal”.

Logo, ao se ver essa teoria associada ao sistema de responsabilidades, pode-se depreender que seu objeto é tutelar a expectativa do consumidor em ver o seu objeto e a relação de consumo a funcionarem corretamente, sem dissabores e/ou danos efetivos.

Por conta disso, pode-se afirmar que essa teoria se aplica à proteção dos dados pessoais, pois, ao ser necessário que essas informações sejam disponibilizadas a terceiros para que a relação de consumo se efetive, o mínimo que se espera é que esses registros sejam utilizados tão-somente para esse fim, e não para situações diversas, que se prestam apenas a fomentar a atividade de fornecedores em detrimento do resguardo necessário ao cidadão-consumidor²⁴.

A partir desse raciocínio, denota-se que o início da proteção de dados se dá com a sua utilização correta, isto é, com seu emprego adequado aos fins a que foi

²⁴ A esse respeito, Pezzi (2007, p. 143) assevera que: “Essa adequação, nos dias atuais, refere-se não somente ao atendimento das especificações do produto ou serviço. Ela vai além. Os fornecedores devem estar atentos à satisfação do cliente, isto é, a concorrência de mercado cria a necessidade de se ter um diferencial, que usualmente está diretamente relacionado com o bem-estar e a satisfação do cliente. O que se busca é a sua lealdade e a sua fidelização como forma de mantê-lo em sua carteira de clientes por muito tempo, tornando-o incorruptível por outras marcas ou modelos. A coleta e o armazenamento de informações da clientela por meio de bancos de dados e cadastros de consumidores deve estar, assim, afinada com esse princípio de modo a evitar que bens jurídicos, como a privacidade, sejam afetados”.

proposto, pois, dessa forma, estar-se-á a garantir a intenção originária do cidadão que disponibiliza os seus dados pessoais.

Com base nessa compreensão, extrai-se, também um dever negativo e outro positivo ao gestor desse banco de dados, quais sejam: o dever de não repassar as informações de que dispõe, sob pena de violar o direito à privacidade dos seus titulares em razão do vício de qualidade/adequação; e o dever de garantir que esses registros não sejam acessados por terceiros estranhos à relação jurídica que embasou o fornecimento dos dados.

Nessa direção, Benjamin (2013, p. 148), *mutatis mutandis*, comenta que:

[...] Enquanto a adequação dos produtos e serviços é uma *condição positiva* imposta ao fornecedor (o consumidor tem uma expectativa afirmativa de adequação), o respeito da segurança do consumidor ocorre como uma *condição negativa* da produção e comercialização no mercado de consumo (o consumidor tem uma expectativa negativa de insegurança).

À vista disso, está claro que o direito básico do consumidor à segurança impõe ao gestor do banco de dados um dever jurídico de se comportar adequadamente, com especial atenção à confidencialidade, integridade e disponibilidade das informações, sob pena de responder patrimonialmente pela falha na segurança (MENDES, 2014).

Em reforço ao disposto no Código de Defesa do Consumidor está o Decreto n. 7.962, de 15 de março de 2013 que, ao regulamentar o aludido código e ao dispor sobre a contratação no comércio eletrônico, renovou e sedimentou o dever/direito básico à segurança.²⁵

Logo, são inquestionáveis o dever e a responsabilidade dos bancos de dados pela segurança das informações, o que deve ser feito ativamente, a todo tempo e por meios técnicos eficientes, já que, dentre as implicações da teoria da qualidade/adequação, está a necessidade que a coleta e o tratamento dos dados sejam feitos com bastante cuidado e correção (BRASIL, 2010).

Para mais, tem-se que o referido decreto, além de reforçar o dever de segurança, fortaleceu algumas garantias constitucionais do cidadão consumidor,

²⁵ Nesse sentido, Miragem (2013, p. 296), esclarece que: “No tocante à segurança dos meios de pagamento e tratamento de dados dos consumidores, o Dec. 7.962/2013, restringe-se a estabelecer um dever dos fornecedores de ‘utilizar mecanismos de segurança eficazes’ (art. 4º, VII). A regra aqui é tautológica, e reproduz o disposto no artigo 45-C, IV, proposto a incluir no DC pelo PLS 281/2012. Especializa, contudo, o óbvio dever de segurança do fornecedor no meio eletrônico”.

pois, ao determinar que a relação jurídica de consumo eletrônico deverá se pautar pelo atendimento facilitado ao consumidor (artigo, 1º, inciso II), verifica-se a necessidade do fornecedor em se disponibilizar a cooperar para com o perfeito adimplemento, o que abrange o integral conhecimento, acesso e controle das informações necessárias à formação e execução do vínculo jurídico e, por consequência, fortalece o princípio da autodeterminação informativa (EFING e CATUZO, 2016).

Em confirmação a este raciocínio, destaca-se a disposição contida no artigo 4º, inciso II, do Decreto n. 7.962/2013, que, ao exemplificar as condutas que o fornecedor deverá tomar para garantir o atendimento facilitado ao consumidor, estabelece a necessidade de disponibilização de instrumentos que possibilitem o adquirente a identificar e corrigir eventuais erros ocorridos anteriormente à contratação.²⁶

No que se refere ao direito básico à informação, previsto no artigo 6º, inciso III, do Código de Defesa do Consumidor, deve-se destacar, de início, que a sua leitura precisa ser feita como a condição necessária à educação do cidadão-consumidor, o que também se caracteriza como um direito básico (artigo 6º, inciso II, do referido Código) e comprova a importância dessa prerrogativa, pois, sem ela, não se pode falar em vontade livre e nem consciente²⁷, o que impede a implementação da autodeterminação informativa e, por conseguinte, nega vigência ao direito à privacidade.

Segundo Marques (2013, p. 73), o direito básico à informação tem por função trazer transparência à relação jurídica a ser realizada, sendo que sua incidência deve ocorrer no momento pré-contratual, durante a sua execução e posteriormente ao seu exaurimento.

²⁶ Apesar da importância da posituação desse regramento, faz-se necessário registrar aqui a discordância quanto a limitação temporal prevista no texto legal, pois, tendo em vista que alguns equívocos podem ocasionar prejuízo à privacidade, não se pode temporalmente limitar a eficácia de um direito fundamental. Além disso, o dever jurídico de segurança, como corolário da boa-fé objetiva, deve se fazer presente em todas as fases da relação jurídica, o que também não se mostra compatível com a previsão temporal prevista na disposição legal.

²⁷ Tendo por base o Recurso Especial n. 1144840/SP, verifica-se que: “O direito à informação visa a assegurar ao consumidor uma escolha consciente, permitindo que suas expectativas em relação ao produto ou serviço sejam de fato atingidas, manifestando o que vem sendo denominado de consentimento informado ou vontade qualificada. Diante disso, o comando do art. 6º, III, do CDC, somente estará sendo efetivamente cumprido quando a informação for prestada ao consumidor de forma adequada, assim entendida como aquela que se apresenta simultaneamente completa, gratuita, útil, vedada, neste último caso, a diluição da comunicação efetivamente relevante pelo uso de informações soltas, redundantes ou destituídas de qualquer serventia para o consumidor”.

Ainda segundo a autora (2013, p. 73), constata-se que o direito básico à informação transpassa a mera formalidade do contrato, uma vez que os dados solicitados ao consumidor ou repassados pelo fornecedor integram a relação jurídica, de modo que, caso ocorra alguma falha, fica evidente o vício de qualidade do produto ou serviço oferecido.

Diante disso, além do direito básico à informação retomar a aplicabilidade da teoria da qualidade/adequação, verifica-se que o seu cumprimento é elementar ao controle de dados pessoais e, logicamente, à autodeterminação informativa, o que torna essa prerrogativa tão essencial à proteção dos dados pessoais, afinal, não fosse esse dever jurídico de transparência, que possui natureza preventiva, a tutela da privacidade, além de extremamente prejudicada, estaria restrita à sua reparação, o que obviamente não é compatível com a prática do solidarismo constitucional.

Nessa direção, Mendes (2014, p. 65) assevera que:

O tratamento de dados pessoais tem como pressuposto a sua completa transparência em relação a quem são os responsáveis e os gestores do tratamento, qual a sua finalidade, qual é a utilização dos dados e que tipos de dados são processados, etc. Sem a devida transparência, torna-se impossível qualquer tipo de controle pelo titular do fluxo de seus dados, assim como qualquer fiscalização pelos órgãos de controle.

Além disso, a autora (2014, p. 65) comenta que:

Isso envolve, com base no art. 6º, III, do CDC, o direito do consumidor de ser informado sobre: (i) quais os dados pessoais serão tratados e para quais finalidades; (ii) se os dados pessoais são transmitidos para terceiros; (iii) para quais países os dados pessoais são transmitidos, se for o caso; (iv) qual é o período de conservação de dados; e (v) quais os mecanismos de segurança utilizados para garantir a segurança dos dados pessoais. Afinal, como determina o artigo 46 do CDC, 'os contratos que regulam as relações de consumo não obrigarão os consumidores, se não lhes for dada a oportunidade de tomar conhecimento prévio de seu conteúdo (...)'. Ademais, por meio da aplicação analógica do art. 31 do CDC, é possível se extrair o dever de que a informação seja fornecida de forma correta, clara, precisa, ostensiva e em língua portuguesa.

Compreendida a essencialidade do direito/dever à informação, impende salientar que a sua efetivação não se dá com a sua simples disponibilização. É preciso mais.

Segundo o artigo 6º, inciso III, do Código de Defesa do Consumidor, a informação a ser prestada é qualificada, isto é, ela deve ser adequada, clara e precisa.

De acordo com Bioni (2014, p. 293) a informação, além de ser útil, precisa crescer, isto é, tem que ser capaz de permitir o destinatário racionalizar suas decisões e lhe possibilitar alcançar uma perspectiva crítica, pois, somente dessa forma o titular dos dados terá condições de conhecer e modificar eventual situação que não seja do seu agrado.

Para mais, ao se considerar que as informações, para efetivamente serem úteis, necessitam ser precisas, cumpre destacar que o excesso informacional também se revela prejudicial, uma vez que não permite a real compreensão por parte do destinatário.

À vista disso, destaca-se que a informação, para ser eficiente à proteção dos dados pessoais, deve ser o suficientemente acessível e apta a esclarecer a função dos dados, a sua destinação, a forma pela qual será feita seu tratamento, quais as medidas de segurança são adotadas e, ainda, quais são os riscos inerentes a essa atividade, pois, dessa forma, estar-se-á a dar azo ao dever jurídico de cooperação entre os sujeitos da relação jurídica e aos direitos constitucionais, haja vista a instrumentalização do titular dos dados pessoais²⁸.

Logo, é inconteste que para proteger informações se faz necessário informar, sobretudo ao se considerar a proteção principiológica trazida pelo Código de Defesa do Consumidor, com especial destaque para a boa-fé objetiva.

Segundo Marques (2013, p. 68) a boa-fé objetiva deve ser compreendida como o fio condutor de toda a tutela trazida pelo Código de Defesa do Consumidor, uma vez que, além de ser cláusula geral de todo o ordenamento jurídico²⁹, a sua

²⁸ A esse respeito, Bioni (2014, p. 293-294) explica que: “Dada a racionalidade limitada (bounded rationality) do ser humano, o excesso de informação, também, desinforma (overloaded information), razão pela qual informação adequada é aquela que permite ao consumidor saber das qualidades características do bem de consumo, e, ainda, a sua utilização atenta aos riscos que lhe pode sobrevir. Verifica-se, dessarte, que a quantidade de informação pode prejudicar a qualidade da informação transmitida. Contudo, tais critérios não se confundem, ainda que haja um ponto de contato entre eles. Pode-se dizer, retomando o que já foi dito, que o critério qualitativo liga-se à ideia de uma informação original e imprevisível que equaliza a disparidade informacional entre consumidor e fornecedor. *A posteriori*, deve-se conectar – num segundo plano – a quantidade de informações transmitidas, se suficientes ou não para revelar ao consumidor um conteúdo para apreensão crítica. Não adianta atentá-lo sobre algo que lhe é útil se o conteúdo informativo não é completo suficiente para nela desencadear uma compreensão completa, e, por último, racionalizar uma tomada de decisão – poder de decisão”.

²⁹ De acordo com Varela (2005, p. 121) a boa-fé objetiva “consistem em um dos princípios gerais do direito solidamente enraizados”.

substancialidade consiste na retidão da conduta, isto é, no dever de agir em prol do melhor adimplemento e das legítimas expectativas dos envolvidos³⁰.

Enquanto princípio, não restam dúvidas de que a boa-fé objetiva tem, dentre suas diversas funções, a capacidade de potencializar a abrangência do regramento, seja por meio da ressignificação de alguns institutos, para coaduná-los com os ditames constitucionais, seja prestando-se como fonte de direitos/deveres jurídicos diversos, afinal, conforme aponta Negreiros (1998, p. 15), o núcleo da boa-fé objetiva reside em ser um mandamento de conduta ativo, ou seja, serve de fundamento à exigência de cumprimento da prestação e dos demais elementos acidentais que circunscrevem a relação jurídica, tal como os dados pessoais.

Não obstante, não se pode deixar de considerar os ensinamentos trazidos por Frada (2007, p. 441-442), segundo o qual a boa-fé objetiva também deve ser compreendida sob uma perspectiva negativa, pois, segundo o autor, esse princípio também se densifica como uma regra de proibição, pela qual se exclui a permissibilidade de atuar contrariamente aos fins da relação jurídica obrigacional.

Ao tratar das funções da boa-fé objetiva a luz do Estado Social e da dignidade humana, Pinheiro (2004, p. 05), destaca quatro funções principais, quais sejam: interpretativa, pela qual deve-se se fazer prevalecer a confiança sobre a vontade e o sentido literal da linguagem³¹; a integrativa, pela qual a boa-fé objetiva serve como fonte de deveres obrigacionais, que acabam por alargar o parâmetro da responsabilidade; a limitadora, pela qual se traçam os limites das condutas e se exercita o controle das posições jurídicas; e a finalística, que resgata a dimensão da interpretação teleológica das relações obrigacionais em favor do equilíbrio e equidade das relações jurídicas.

Para este trabalho, merecem destaque as funções integrativa e limitadora, pois, desses arcabouços jurídicos é possível extrair, além do dever jurídico de informação acima descrito, o princípio da confiança, veracidade e finalidade dos dados pessoais.

Em relação à função integrativa, Negreiros (1998, p. 91), ao analisá-la sob a perspectiva do direito civil-constitucional, destaca que a boa-fé objetiva tem por

³⁰ Segundo Nalin (2003, p. 27): “não me parece concebível uma boa-fé objetiva destituída de intencionalidade e, logo, de crença (psicológica) de que está procedendo conforme a ética, sem violar o interesse alheio e a ordem jurídica”.

³¹ Art. 112 do Código Civil. Nas declarações de vontade se atenderá mais à intenção nelas consubstanciada do que ao sentido literal da linguagem.

fundamento a dignidade humana e, em razão disso, esse princípio faz surgir um dever de cooperação, pelo qual a solidão contratual dá lugar à solidariedade obrigacional.

Diante disso, depreende-se que não cabe aos sujeitos da relação jurídica atuarem da forma que bem entenderem, uma vez que a sua conduta se encontra limitada pela segurança dos interesses alheios.

Ao transpor essa colocação à proteção jurídica dos dados pessoais, destaca-se que o gestor do banco de dados não tem liberdade de dispor dessas informações da maneira que melhor lhe aprouver ou for mais rentável, em detrimento dos direitos do outro sujeito que fez parte dessa relação. Pelo contrário, cabe ao controlador dos dados cooperar para com a segurança dos titulares dos dados, o que pode ser feito pela disponibilização de meios de controle e mediante a busca do assentimento do sujeito para com o tratamento das suas informações para além da finalidade pela qual as disponibilizou.

A partir desses apontamentos, ressalta-se, por sua vez, a função limitadora da boa-fé objetiva, que, ao ter por escopo vedar a prática de condutas juridicamente patológicas, relaciona-se intimamente ao abuso de direito, mais especificamente, como fundamento da responsabilidade por esse tipo de ato ilícito.

À vista disso, destaca-se que o tratamento inadequado dos dados pessoais se caracteriza como abuso de direito, afinal, com base no artigo 187 do Código Civil³², não restam dúvidas que o repasse de dados pessoais a terceiros, sem a anuência do titular, ultrapassa a finalidade econômica anteriormente esperada e consentida.

Logo, é inconteste que a boa-fé objetiva, como padrão de conduta a ser seguido pelos sujeitos da relação jurídica obrigacional, consiste em um poderoso instrumento jurídico de proteção aos dados pessoais.

Compreendidas algumas das ferramentas de proteção estabelecidas pelo Código de Defesa do Consumidor e pelo Decreto 7.962/2013, os quais possuem inequívoca aplicabilidade no âmbito das relações jurídicas de consumo em meio eletrônico, passa-se, nesse momento, à análise de alguns dos dispositivos protetivos

³² Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes.

presentes na Lei n. 12.965/2014, popularmente conhecida como Marco Civil da Internet.

Impende ressaltar que essa legislação possui grande relevância no contexto da sociedade da informação, pois, ao estabelecer os princípios, direitos e deveres do uso da internet no Brasil, amplia o espectro da proteção dos dados pessoais para além das relações de consumo firmadas em meio eletrônico. É dizer: devido ao caráter geral desse corpo normativo, a sua proteção incide sobre qualquer relação firmada em meio eletrônico, seja ela de consumo ou meramente social.

Ao se iniciar a análise dessa lei, destaca-se, de início, os artigos 2º, inciso II, e 3º, inciso II e III, pelos quais se observa a preocupação do legislador para com a privacidade e os dados pessoais.

No corpo desses dispositivos legais, verifica-se que um dos fundamentos do uso da internet no Brasil é o desenvolvimento da personalidade humana e o exercício da cidadania em meios digitais, o que se conecta ao direito fundamental à privacidade, afinal, não se pode compreender o desenvolvimento humano dissociado da reserva do seu âmbito particular.

Segundo Fiorillo (2015, p. 29), o desenvolvimento da personalidade requer a possibilidade de se autodeterminar, o que compreende o controle sobre o grau da sua preservação e/ou exposição e, mais uma vez, denota a importância da autodeterminação informativa como mecanismo fundamental ao direito à privacidade e à proteção dos dados pessoais na sociedade da informação, pois, tendo em mente a dinamicidade do meio, apenas o controle realizado mediante a manifestação da individualidade do sujeito é apto a garantir a proteção a esses direitos e o desenvolvimento desimpedido dos cidadãos.

Juntamente a esses dispositivos, a lei do Marco Civil da Internet, em seu artigo 7º, inciso VII, positiva como direito ao usuário de internet no Brasil o “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” o que consiste, por sua vez, na dimensão ativa do direito fundamental à privacidade, isto é, na autodeterminação informativa.

Segundo Paesani (2014, p. 521), tem-se, por esse dispositivo legal, uma objetivação do direito à privacidade, que ocorre por meio dos dados pessoais, uma vez que essas informações são capazes de identificar certas características do

sujeito mesmo quando ele é analisado fora do seu contexto social e cultural, o que ocorre a todo tempo quando se está a falar do meio eletrônico, razão pela qual a autodeterminação informativa se faz como mecanismo necessário à proteção das informações pessoais.

Ainda segundo a autora:

O direito ao não fornecimento dos dados a terceiros se manifesta como ampliação do princípio do consentimento do direito à autodeterminação informativa, de origem germânica, que disponibiliza ao indivíduo determinar quanto e quais dados quer expor. E, estendendo a interpretação do princípio, firma-se a possibilidade de negar a terceiros o acesso aos seus dados pessoais. Identifica-se, nesses casos, o caráter democrático do sistema [...]. Este inciso delega ao usuário amplo poder de controle sobre as informações que o identificam.

Diante dessa colocação, está evidente que a autodeterminação informativa se mostra como o principal instrumento de controle sobre o fluxo informacional disponibilizado no contexto da sociedade da informação.

Não obstante, faz-se necessário comentar que, embora esse princípio resida no mandamento constitucional do direito à privacidade, a efetivação da proteção dos dados pessoais no âmbito da sociedade da informação possui diversos outros fundamentos jurídicos, que se amparam em disposições legais, as quais, somadas ao texto constitucional, criam uma proteção sistêmica contundente, como se verá no capítulo a seguir.

4 ANÁLISE SISTÊMICA DA PROTEÇÃO JURÍDICA AOS DADOS PESSOAIS E A SUA APLICAÇÃO PELOS TRIBUNAIS

Como visto nos capítulos anteriores, a sociedade da informação, em razão da agilidade com que se move e da sua complexidade, exige uma ressignificação de alguns institutos jurídicos para que sua eficácia possa atingir e absorver situações fáticas antes não pensadas pelo legislador, o que requer, de saída, a verticalização dos conceitos normativos e a sua análise conjunta às demais regras de proteção.

À vista disso, ao se ter por base o direito fundamental à privacidade, verifica-se que a sua dimensão individualista não se faz mais suficiente para albergar o cidadão do nível de exposição trazido pela sociedade da informação, que, ao se alimentar dos registros sociais disponibilizados cotidianamente, é capaz de objetivar o perfil do sujeito e colocá-lo em uma condição de constante monitoramento.

Em razão disso, ganha efeito a dimensão social da privacidade, a qual, ao também se amparar no solidarismo constitucional, previsto como um objetivo da república, serve de fundamento lógico-jurídico às regras infraconstitucionais de proteção, especialmente ao direito à segurança, à informação e ao princípio da boa-fé objetiva.

Para além da sua dimensão social, o direito fundamental à privacidade, ao ser lido a partir da sua eficácia horizontal, também se mostra como o fundamento jurídico de apoio à boa-fé objetiva, mormente em relação à sua função limitadora, pois, a partir dessa dimensão, tem-se definido os novos limites da gestão privada dos dados pessoais, os quais, apesar de poderem ser contornados mediante os instrumentos de segurança corretos, jamais poderão ser suprimidos.

Logo, é inconteste que o conteúdo disposto na Constituição Federal é mais que suficiente para proteger o cidadão dos riscos inerentes aos novos contextos, afinal, a isso se presta a mutação constitucional.³³

No entanto, embora os direitos fundamentais sejam disposições jurídicas de proteção por excelência e possuam aplicabilidade imediata, não se pode deixar de mencionar que as regras infraconstitucionais são capazes de trazer maior

³³ De acordo com Mendes e Branco (2012, p. 152): “Ocorre que, por vezes, em virtude de uma evolução na situação de fato sobre a qual incide a norma ou ainda por força de uma nova visão jurídica que passa a predominar na sociedade, a Constituição muda, sem que as suas palavras hajam sofrido modificação alguma. O texto é o mesmo, mas o sentido que lhe é atribuído é outro. Como a norma não se confunde com o texto, repara-se, aí, uma mudança da norma, mantida o texto. Quando isso ocorre no âmbito constitucional, fala-se em mutação constitucional”.

concretude ao direito, principalmente quando são formuladas por meio de microssistemas e direcionados a um recorte social específico.

É nesse sentido que se faz, agora, uma análise integrativa do Código de Defesa do Consumidor, que, ao representar o início de uma adequação das relações civis aos parâmetros constitucionais, coloca à disposição da sociedade os direitos básicos à segurança, informação e transparência, os quais, a propósito, mostram as diversas perspectivas do princípio da boa-fé objetiva.

Sob o manto dessa legislação, que parte da premissa da vulnerabilidade do consumidor, especialmente quando inserido em um novo meio - tal como o da sociedade da informação -, torna-se evidente a proeminência de um dever jurídico de cooperação, afinal, é o fornecedor - e, por conseguinte - o gestor do banco de dados que, por conta da superioridade técnica e informacional, tem condições de melhor garantir os objetivos e interesses dos consumidores, o que deve ser feito, logicamente, com o respeito aos limites da vontade manifestada.

Em complemento a esse regramento, tem-se o Decreto n. 7.962/2013, que, ao restringir a sua incidência ao âmbito do comércio eletrônico, reforça a potencialização da vulnerabilidade do consumidor nesse meio, motivo pelo qual atribui aos fornecedores um dever de cuidado ainda maior para com a segurança do cidadão-consumidor, haja vista que esse corpo normativo traz um acautelamento ainda maior da vontade emitida pelo sujeito.

Nesse cenário, não restam dúvidas que o Código de Defesa do Consumidor e o Decreto n. 7.962/2013 se prestam a formar uma ponte entre a proteção constitucional aos dados pessoais e o comércio eletrônico, afinal, na medida em que essas legislações buscam a regulamentar essa situação de fato em compatibilidade à Constituição Federal, tem-se o resgate de um estado de coisas inconstitucional, o que se faz necessário à eficácia imediata dos direitos fundamentais.

No que concerne ao Marco Civil da Internet, tem-se a positivação do princípio da autodeterminação informativa, o que, sem dúvida, consiste na busca da efetividade da dimensão positiva do direito à privacidade, haja vista que essa legislação se apresenta absolutamente consentânea aos riscos trazidos por esse contexto da fluidez digital, os quais, para serem amenizados, exigem, para além da concretização de um dever jurídico de cooperação por parte do gestor dos dados pessoais, a possibilidade de um controle social ativo.

Tendo em vista essa contextualização jurídica, pode se afirmar que, para que se garanta a privacidade necessária ao desenvolvimento da personalidade humana, a proteção dos dados pessoais deve ser encarada como uma obrigação coletiva, pela qual os cidadãos, os entes privados e o Estado atuem de forma colaborativa em prol do equilíbrio almejado pelo texto constitucional, que prevê a coexistência de direitos fundamentais negativos aos princípios necessários para o desenvolvimento das relações jurídico-econômicas, tal como livre concorrência e livre iniciativa, os quais, apesar de justificarem a formatação de bancos de dados como instrumentos catalisadores das relações econômicas, não os isenta de limites.

Nota-se, com isso, que os dados pessoais no âmbito da sociedade da informação possuem proteção jurídica contundente. Todavia, nem sempre os seus instrumentos são devidamente aplicados pelos Tribunais, que, no mais das vezes, sucumbem ao poderio do crédito e não vislumbram a ocorrência de dano moral quando há o repasse de informações pessoais a terceiros para que seja feita uma análise de risco financeiro, o que é chamado de *credit scoring*³⁴.

Ao analisar essa prática mercadológica, o Ministro Paulo de Tarso Sanseverino, no julgamento do Recurso Especial n. 1.419.697/RS, considerou-a lícita, sob a justificativa de que o repasse de informações para análise de riscos não constitui um banco de dados, mas apenas uma avaliação estatística.³⁵

Não obstante, o Ministro condicionou a prática dessa atividade à observância do direito à privacidade e à proteção do consumidor, embora tenha entendido que o consentimento do cidadão não se faz necessário a esse tipo de avaliação.

³⁴ Com base no voto do Ministro Paulo de Tarso Sanseverino no julgamento do Recurso Especial n. 1.419.697/RS (2014, p. 8), “o chamado *credit scoring* ou simplesmente *credscore* é um sistema de pontuação do risco de concessão de crédito a determinado consumidor. Trata-se de um método desenvolvido para avaliação do risco de concessão de crédito a partir de modelos estatísticos, considerando diversas variáveis de decisão, com atribuição de uma nota ao consumidor avaliado conforme a natureza da operação a ser realizada. [...]. As ‘variáveis de decisão’ são fatores que a experiência empresarial denotou como relevantes para avaliação do risco de retorno do crédito concedido. Cada uma dessas variáveis recebe uma determinada pontuação, atribuída a partir de cálculos estatísticos, formando a nota final. Consideram-se informações acerca do adimplemento das obrigações (histórico de crédito), assim como os dados pessoais do consumidor avaliado (idade, sexo, estado civil, profissão, renda, número de dependentes, endereço)”.

³⁵ “O fato de se tratar de uma metodologia de cálculo do risco de concessão de crédito, a partir de modelos estatísticos, que busca informações em cadastros e bancos de dados disponíveis no mercado digital, não afasta o dever de cumprimento desses deveres básicos, devendo-se apenas ressaltar dois aspectos: De um lado, a metodologia em si de cálculo da nota de risco de crédito (“*credit scoring*”) constitui segredo da atividade empresarial, cujas fórmulas matemáticas e modelos estatísticos naturalmente não precisam ser divulgadas (art. 5º, IV, da Lei 12.414/2011: ...“resguardado o segredo empresarial”). De outro lado, não se pode exigir o prévio e expresso consentimento do consumidor avaliado, pois não constitui um cadastro ou banco de dados, mas um modelo estatístico” (2014, p. 34).

Além disso, o Ministro, em seu voto (2014, p. 36), declarou que “para a caracterização do dano extrapatrimonial, há necessidade de comprovação de uma efetiva recusa de crédito, com base em uma nota de crédito baixa, por ter sido fundada em dados incorretos ou desatualizados”.

Nessa mesma direção, tem-se o seguinte julgado paranaense:

PODER JUDICIÁRIO DO ESTADO DO PARANÁ 1ª TURMA RECURSAL - PROJUDI Rua Mauá , 920 - 28º andar - Alto da Glória - Curitiba/PR - CEP: 80.030-200 - Fone: 3017-2568 Autos nº. 0002877-48.2013.8.16.0126 Recurso: 0002877-48.2013.8.16.0126 Classe Processual: Recurso Inominado Assunto Principal: Inclusão Indevida em Cadastro de Inadimplentes Recorrente (s): COMÉRCIO DE ALIMENTOS RONDONENSE LTDA Recorrido (s): PEREIRA 2) Inocorrência de violação ao art. 535, II, do CPC. 3) Não reconhecimento de ofensa ao art. 267, VI, e ao art. 333, II, do CPC. 4) Acolhimento da alegação de inocorrência de dano moral "in re ipsa". 5) Não reconhecimento pelas instâncias ordinárias da comprovação de recusa efetiva do crédito ao consumidor recorrido, não sendo possível afirmar a ocorrência de dano moral na espécie. 6) Demanda indenizatória improcedente. III ? NÃO CONHECIMENTO DO AGRAVO REGIMENTAL E DOS EMBARGOS DECLARATÓRIOS, E RECURSO ESPECIAL PARCIALMENTE PROVIDO. (REsp 1419697/RS, Rel. Ministro PAULO DE TARSO, SANSEVERINO, SEGUNDA SEÇÃO, julgado em 12/11/2014, DJe 17/11/2014). **Assim sendo, considerando o entendimento assentado pela Corte Superior no sentido de que tal prática comercial não se trata de um cadastro ou banco de dados (e sim de uma metodologia de cálculo de risco de crédito), não há que se falar em condenação ao pagamento de indenização por danos morais, bem como em exclusão dos dados do consumidor do sistema ,concentre scoring na medida em que não há necessidade do consentimento do consumidor (a) para a divulgação dos dados discutidos na lide, situação portanto que não viola o direito personalíssimo.** Curitiba, data da assinatura eletrônica. Aldemar Sternadt Magistrado (TJPR - 1ª Turma Recursal - 0002877-48.2013.8.16.0126/0 - Palotina - Rel.: Aldemar Sternadt - - J. 25.01.2016) (TJ-PR - RI: 000287748201381601260 PR 0002877-48.2013.8.16.0126/0 (Decisão Monocrática), Relator: Aldemar Sternadt, Data de Julgamento: 25/01/2016, 1ª Turma Recursal, Data de Publicação: 25/01/2016) (grifo nosso).

Diante dessas decisões, impende salientar, de antemão, que não é esse o entendimento defendido nesse trabalho, uma vez que, dentre diversos outros fatores, a simples mudança do nome da atividade não é o suficiente para desnaturá-la. É dizer: embora a jurisprudência afirme que essa análise de crédito não se revista do caráter de banco de dados, a realidade, aparentemente, aponta em sentido diverso, afinal, o que é a reunião de dados específicos dirigidos a um fim predeterminado?

Para mais, a não exigência do consentimento do consumidor para a realização do *credit scoring*, além de ser invasivo à sua privacidade, pode colocá-lo

em situação de constrangimento que vai muito além do mero dissabor da vida cotidiana, tendo em vista que o resultado dessa avaliação velada dos dados pessoais, indubitavelmente, é capaz de frustrar qualquer expectativa de crédito e, conseqüentemente, da realização de alguns projetos³⁶.

Juntamente a isso, a desnecessidade da anuência do consumidor para com o repasse dos seus dados simplesmente ignora a dimensão ativa do direito à privacidade, isto é, a autodeterminação informativa, o que, por consequência, coloca o cidadão-consumidor em uma condição de vulnerabilidade acentuada, haja vista que seu perfil econômico-financeiro está a ser desenhado sem a consulta e a possibilidade de interferência do principal interessado, que, logicamente, é o titular dos dados.

Em acréscimo, constata-se que a prática do *credit scoring*, nos termos acima delineados, rejeita também a perspectiva social do direito à privacidade e a boa-fé objetiva, uma vez que essa prática não denota um padrão de conduta altruísta, em consonância ao solidarismo constitucional. Pelo contrário. A referida atividade se mostra como um claro exemplo de sobreposição dos interesses individuais ao coletivo, da segurança patrimonial em detrimento do bem-estar social.

Nesse sentido e, portanto, contrário ao posicionamento adotado pelo Superior Tribunal de Justiça e pelo Tribunal de Justiça do Paraná, segue uma decisão do Tribunal de Justiça do Rio Grande do Sul:

AGRAVO EM APELAÇÃO CÍVEL. Responsabilidade civil. Ação cominatória de obrigação de fazer cumulada com indenizatória por dano moral. SERASA. *CONCENTRE SCORING*. ILEGALIDADE DO SERVIÇO. DIREITO À INFORMAÇÃO. VIOLAÇÃO. **É abusiva a prática comercial de utilizar dados negativos dos consumidores, para lhe alcançar uma pontuação, de forma a verificar a probabilidade de inadimplemento.** Sem dúvidas, este sistema não é um mero serviço ou ferramenta de apoio e proteção aos fornecedores, como quer fazer crer a demandada, mas uma forma de burlar direitos fundamentais, afrontando toda a sistemática protetiva do consumidor, que inegavelmente se sobrepõe à proteção do crédito. Reconhecer a ilicitude deste serviço não significa uma forma de proteção aos maus pagadores. Estes já contam com seu nome inscrito nos órgãos de proteção ao crédito, cujos dados podem ser utilizados livremente pelas empresas. O que não é possível é a utilização de registros pessoais dos consumidores, para formar um novo sistema de probabilidade de inadimplemento, sem informar claramente aos interessados e a toda sociedade quais são exatamente as variáveis utilizadas e as razões pelas

³⁶ Nessa direção, Efing (2012, p. 422) comenta que: “[...] a concessão de crédito, sendo relação de confiança, não pode ser atingida por informação injustificada ou inverídica. Destarte, revela-se extremamente relevante o papel dos bancos de dados e cadastros dos consumidores, ainda mais que tais agentes são responsáveis pela possibilidade do consumidor de obter o crédito ou não”.

quais uma pessoa é classificada como com “alta probabilidade de inadimplência” e outra com “baixa probabilidade de inadimplência”. **A falta de transparência e de clareza desta “ferramenta” é incompatível com os mais mezinhos direitos do consumidor. Na forma com que é utilizado o sistema, certamente gera os danos morais alegados na inicial, pois o consumidor que necessita do crédito, negado em face de sua pontuação, fica sem saber as razões pelas quais é considerado propenso ao inadimplemento, restando frustrada legítima expectativa de ter acesso aos seus dados e a explicações sobre a negativa do crédito.** (TJ-RS - Agravo: 70051914893 RS, Relator: Marilene Bonzanini Bernardi, Data de Julgamento: 14/11/2012, Nona Câmara Cível, Data de Publicação: Diário da Justiça do dia 20/11/2012) (grifo nosso).

Não bastassem esses apontamentos, destaca-se, ainda, o condicionamento feito pelo Ministro Paulo de Tarso Sanseverino quando do não reconhecimento do dano moral, sob a justificativa de que o prejuízo à parte interessada pressupõe uma rejeição de crédito decorrente de uma avaliação ruim, feita com base em dados incorretos ou desatualizados.

Como visto acima, não são apenas os dados incorretos que são capazes de causar prejuízo ao cidadão-consumidor, mas também o tratamento inadequado das informações verdadeiras, até porque, essas sim são aptas a causar um verdadeiro prejuízo, uma vez que, ao serem utilizadas incorretamente, não subsiste ao sujeito a possibilidade de se retornar ao *status quo*, por ser impossível alterar a realidade fática, de modo que a sua tutela fica restrita à reparação pecuniária.

Logo, tendo por base os fundamentos que foram apontados no decorrer deste trabalho, pode-se afirmar que a legislação brasileira fornece aos cidadãos diversos mecanismos de proteção jurídica aos dados pessoais. No entanto, essas ferramentas não são integralmente utilizadas no cotidiano forense, pois, ao que se constata, sempre há um ponto a ser relativizado.

Em todo caso, o fato é que a desproteção ou o abuso da utilização dos dados pessoais, quando ocorrem, não são decorrentes da ausência de legislação, mas sim da sua interpretação fragmentada, isto é, concentrada na expansão econômica em detrimento do desenvolvimento humano (EFING, 2012).

5 CONCLUSÃO

Conhecidas as características da sociedade da informação, pode-se observar que o registro de dados pessoais por meio eletrônico é um instrumento elementar à propulsão dessa nova perspectiva sociológica.

Além dos mais, verifica-se que essa estrutura social, pautada pelos mecanismos digitais, em muito facilita o cotidiano dos cidadãos-consumidores, afinal, é evidente a ampliação do acesso a bens e serviços disponíveis para além das barreiras geográficas.

Em contrapartida, a vulnerabilidade dos sujeitos também é potencializada, o que justifica, por conseguinte, uma releitura dos mecanismos jurídicos de proteção em busca da segurança efetiva dos dados pessoais no contexto da sociedade da informação.

À vista disso, observa-se que a reinterpretação do corpo normativo se inicia dentro e a partir da Constituição Federal, com base em uma nova dimensão do direito à privacidade, que deixa de se referir apenas a um não fazer e passa a ser fonte de mecanismos ativos de proteção, que são o controle social da privacidade e a autodeterminação informativa, os quais se mostram consentâneos ao objetivo da República em se construir uma sociedade livre, justa e solidária.

Para mais, ao se ter a proteção do consumidor como um direito fundamental e como princípio da ordem econômica, constata-se, aqui, o primeiro fundamento da vulnerabilidade do cidadão-consumidor, o que justifica a aplicação de mecanismos sistêmicos em sua proteção, os quais devem ser considerados e aplicados pelas perspectivas vertical e horizontal dos direitos e garantias fundamentais.

Sob o manto da proteção infraconstitucional, ressalta-se que a proteção jurídica aos dados pessoais se dá com o Código de Defesa do Consumidor, com o Decreto n. 7.962/2013 e com a Lei n.12.965/2014, que criou o Marco Civil da Internet.

Com base nesse arcabouço legislativo, verifica-se que por conta de um dever jurídico de cooperação em favor da segurança, uma dimensão finalística dos dados pessoais ganha efeito, pois, com base na boa-fé objetiva, que se mostra como princípio geral, pode-se notar a necessidade de se utilizar os dados pessoais nos limites da finalidade pelo qual foram disponibilizados pelo seu titular, o que se mostra como uma obrigação de cunho negativo.

Não obstante, é importante destacar que a positivação da autodeterminação informativa, em contraponto ao dever negativo acima entabulado, confere uma dimensão positiva ao direito fundamental à privacidade, haja vista que esse instrumento intenciona colocar nas mãos do titular dos dados o controle efetivo sobre suas informações.

Diante desse cenário, nota-se, apesar da existência de um aparato normativo apto a garantir a proteção de dados pessoais em meio eletrônico, que nem sempre o ordenamento jurídico é apreciado em sua inteireza, o que dá margem à apreciação utilitarista dos mecanismos de proteção aos registros de dados, a qual, no mais das vezes, acontece em favor do poderio econômico em detrimento das garantias individuais, como se verifica de algumas decisões judiciais.

A despeito disso, ainda que os Tribunais assim não reconheçam, o fato é que a relativização de alguns conceitos não altera a solidez legislativa existente em favor da proteção dos dados pessoais, que se perfaz em um dever jurídico coletivo amparado em normas de ordem pública e, portanto, indeclináveis, razão pela qual devem ter o seu cumprimento continuamente exigido.

Diante dessa conjuntura, tem-se, em um apanhado geral, que a proteção jurídica aos dados pessoais no contexto da sociedade da informação se faz de modo colaborativo – que, a propósito, possui fundamentação lógica-jurídica em todos os níveis legislativos -, pois, dessa maneira, é possível compatibilizar o respeito aos direitos fundamentais com os princípios que regem as relações econômicas e sociais, ainda que os órgãos jurisdicionais assim não entendam.

REFERÊNCIAS

ASCENSÃO, José de Oliveira de. **Estudos sobre direito da internet e da sociedade de informação**. Coimbra: Almedina, 2001, p. 46.

BAUMAN, Zygmunt. **Vida para consumo**: a transformação das pessoas em mercadoria. Rio de Janeiro: Zahar, 2008.

BENJAMIN, Antônio Herman V. Teoria da Qualidade. In: BENJAMIN, Antônio Herman V.; MARQUES, Cláudia Lima; BESSA, Leonardo Roscoe. **Manual de direito do consumidor**. São Paulo: Revista dos Tribunais, 2013.

BIONI, Bruno Ricardo. O dever de informar e a teoria do diálogo das fontes para a aplicação da autodeterminação informacional como sistematização para a proteção dos dados pessoais dos consumidores: convergências e divergências a partir da análise da ação coletiva promovida contra o Facebook e o aplicativo 'Lulu'. **Revista de Direito do Consumidor**, São Paulo, v. 94, p. 283-326, 2014.

BRASIL. Código de Defesa do Consumidor: Lei 8.078. **Diário Oficial da União**, 11 de setembro de 1990, Brasília, 1990.

BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial da União**, 5 de outubro de 1988, Brasília, 1988.

BRASIL. Decreto n, 7.962. **Diário Oficial da União**, 15 de março de 2013, Brasília, 2013.

BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Brasília, 2010. Disponível em: <<http://www.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf>>. Acesso em 28 set. 2016.

BRASIL. Lei n. 12.527. **Diário Oficial da União**, 18 de novembro de 2011, Brasília, 2011.

BRASIL. Lei n. 12.965. **Diário Oficial da União**, 23 de abril de 2014, Brasília, 2014.

CASTELLS, Manuel. **The information age: economy, society and culture**. The rise of the network society. Oxford: Blackwell Publishing, 2000.

CASTELLS, Manuel. **A galáxia da Internet**. Reflexões sobre a internet, os negócios e a sociedade. Tradução de Maia Luiza X. de A. Borges. Rio de Janeiro: Zahar, 2003.

CASTRO, Catarina Sarmiento e. **Direito da informática, privacidade e dados pessoais**. Coimbra: Almedina, 2005.

CASTRO, Catarina Sarmiento e. **O direito à autodeterminação informativa e os novos desafios gerados pelo direito à liberdade e à segurança no pós 11 de Setembro**. 2011. Disponível em: <<http://www.buscalegis.ufsc.br/revistas/files/anexos/5544-5536-1-PB.pdf>>. Acesso em: 28 set. 2016.

E-BIT. **Webshoppers 33ª edição 2016**. Disponível em: <http://img.ebit.com.br/webshoppers/pdf/33_webshoppers.pdf>. Acesso em: 15 out. 2016.

EFING, Antônio Carlos. **Banco de dados e cadastro de consumidores**. São Paulo: Revista dos Tribunais, 2002.

EFING, Antônio Carlos. **Contratos e procedimentos bancários à luz do código de defesa do consumidor**. São Paulo: Revista dos Tribunais, 2012.

EFING, Antônio Carlos; CATUZO, Murilo Euler. A proteção jurídica dos dados pessoais na internet. In: **Revista internacional consinter de direito**, Lisboa, ano II, n. II, p.323-342, 1º sem. 2016.

EIRAS, Agostinho. **Segredo de Justiça e controlo de dados pessoais informatizados**. Coimbra: Coimbra, 1992.

FRADA, Manuel António Carneiro da. **Teoria da Confiança e responsabilidade civil**. Coimbra: Almedina, 2007.

GERMAN, Christiano. **O caminho do Brasil rumo à era da informação**. São Paulo: Konrad-Adenauer, 2000.

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2012.

LIMBERGER, Têmis. MORAES, Carla Andreatta Sobbé. A vulnerabilidade do consumidor pela (des)informação e a responsabilidade civil dos provedores na Internet. **Revista de direito do Consumidor**, São Paulo, v. 97, p. 255-270, 2015.

MARQUES, Cláudia Lima. Introdução ao direito do Consumidor. In: BENJAMIN, Antônio Herman V.; MARQUES, Cláudia Lima; BESSA, Leonardo Roscoe. **Manual de direito do consumidor**. São Paulo: Revista dos Tribunais, 2013.

MARQUES, Cláudia Lima. A lei 8.078/90 e os direitos básicos do consumidor. In: BENJAMIN, Antônio Herman V.; MARQUES, Cláudia Lima; BESSA, Leonardo Roscoe. **Manual de direito do consumidor**. São Paulo: Revista dos Tribunais, 2013.

MENDES, Gilmar Ferreira. BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. São Paulo: Saraiva, 2012.

MENDES, Laura Schertel. O direito básico do consumidor à proteção de dados pessoais. **Revista de direito do consumidor**, São Paulo, v. 23, p. 53-75, set. 2014.

MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO. Instituto Brasileiro de Geografia e Estatística (IBGE). **Pesquisa Nacional por Amostra de Domicílios (PNAD 2013)**: tecnologia: acesso à internet. Rio de Janeiro, 2015. Disponível em:

<<http://biblioteca.ibge.gov.br/index.php/bibliotecacatalogo?view=detalhes&id=294414>>. Acesso em: 3 abr. 2016.

MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO. Instituto Brasileiro de Geografia e Estatística (IBGE). **Pesquisa Nacional por Amostra de Domicílios (PNAD 2016):** Acesso à internet e à televisão e posse de telefone móvel celular para uso pessoal, 2016. Disponível em: <<http://biblioteca.ibge.gov.br/visualizacao/livros/liv95753.pdf>>. Acesso em 9 abr. 2016.

MIRAGEM, Bruno. Aspectos característicos da disciplina do comércio eletrônico de consumo: comentários ao Dec. 7.962, de 15.03.2013. **Revista de direito do consumidor**, São Paulo, v. 22, p. 287-300, mar. 2013.

NALIN, Paulo. **A boa-fé como elemento de existência do negócio jurídico.** (Ensaio doutrinário), Curitiba, 2003.

NEGREIROS, Teresa. **Fundamentos para uma interpretação constitucional do princípio da boa-fé.** Rio de Janeiro, Renovar: 2008.

PEZZI, Ana Paula Jacobus. **A necessidade de proteção dos dados pessoais nos arquivos de consumo:** em busca da concretização do direito à privacidade. 2007. 215 f. Dissertação (mestrado) – Universidade do Vale do Rio dos Sinos, São Leopoldo, 2007.

PINHEIRO, Rosalice Fidalgo. **Percorso Teórico da boa-fé objetiva e sua recepção jurisprudencial no direito brasileiro.** 2004. 378 f. Tese (Doutorado) – Universidade Federal do Paraná, Curitiba, 2004.

RODOTÀ, Stefano. **Tecnologie e diritti.** Bologna: Mulino, 1995.

SILVA, José Afonso da. **Curso de direito constitucional positivo.** São Paulo: Malheiros, 2013.

STJ, REsp n. 1419697/RS, 2ª Turma, Relator Ministro Paulo de Tarso Sanseverino, julgado em 12.11.2014, DJe 17.11.2014.

STJ, REsp n. 1144840/SP, 3ª Turma, Relatora Ministra Nancy Andrighi, julgado em 20.03.2012, DJe 11.04.2012.

TJPR, 1ª Turma Recursal, autos n. 0002877-48.2013.8.16.0126/0, Relator: Aldemar Sternadt, julgado em 25.01.2016, publicado em 25.01.2016.

TJRJ, Apelação Cível n. 01933826720118190001, Décima Sétima Câmara Cível, Relator: Elton Martinez Carvalho Leme, julgado em 25.09.2013, Diário da Justiça do dia 22.10.2013.

TJRS, Agravo n. 70051914893, Nona Câmara Cível, Relatora: Marilene Bonzanini Bernardi, julgado em 14.11.2012, Diário da Justiça do dia 20.11.2012.

TJRS, Apelação Cível n. 70061072203, Quinta Câmara Cível, Relatora: Maria Cláudia Cachapuz, julgado em 27/02/2015, Diário da Justiça do dia 02.03.2015.

TJRS, Apelação Cível n. 70060085438, Quinta Câmara Cível, Relatora: Maria Cláudia Cachapuz, julgado em 06/02/2015, Diário da Justiça do dia 18.02.2015.

TOMÉ, Hermínia Campuzano. **Vida privada y datos personales:** su protección jurídica frente a la sociedad de la información. Madrid: Tecnos, 200, p.19-20.

UNIÃO EUROPEIA. Parlamento Europeu e do Conselho. **Directiva 95/46/CE**, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_pt.pdf>. Acesso em 28 set. 2016.

VARELA, João de Matos Antunes. **Das Obrigações em geral**. Coimbra: Almedina, 2005.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade de informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação.** 2007. 296 f. Dissertação (Mestrado) – Universidade de Brasília, Brasília, 2007.