CENTRO UNIVERSITÁRIO DO ESTADO DO PARÁ
ÁREA DE CIÊNCIAS SOCIAIS APLICADAS
CURSO DE BACHARELADO EM DIREITO

Ana Beatriz Henriques de Oliveira

A RESPONSABILIDADE CIVIL NO TRATAMENTO DE DADOS PESSOAIS DE CONSUMIDORES NOS CONTRATOS DE *E-COMMERCE* À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS (LEI Nº 13.709/2018)

Belém
2019

Ana Beatriz Henriques de Oliveira

A RESPONSABILIDADE CIVIL NO TRATAMENTO DE DADOS PESSOAIS DE CONSUMIDORES NOS CONTRATOS DE *E-COMMERCE* À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS (LEI Nº 13.709/2018)

Trabalho de Curso (TC) apresentado como requisito parcial para obtenção do grau de Bacharel em Direito, do Centro Universitário do Estado do Pará (CESUPA).

Orientador: Prof. Dr. Dennis Verbicaro Soares

Belém

2019

Ana Beatriz Henriques de Oliveira

A RESPONSABILIDADE CIVIL NO TRATAMENTO DE DADOS PESSOAIS DE CONSUMIDORES NOS CONTRATOS DE *E-COMMERCE* À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS (LEI Nº 13.709/2018)

Monografia apresentada como requisito parcial para obtenção do título de bacharel em Direito do Centro Universitário do Estado do Pará (CESUPA).

Banca examinadora:

Apresentado em: ___/___/___

_____ - Orientador
Prof. Dr. Dennis Verbicaro Soares
Centro Universitário do Estado do Pará

_____ - Examinador (a)
Centro Universitário do Estado do Pará

À minha família.

AGRADECIMENTOS

Meus primeiros e mais importantes agradecimentos vão aos meus pais Patrícia e Heitor; palavras não bastarão para agradecer a criação que eu recebi de vocês, a educação, a tolerância, apoio e amor que vocês sempre me deram ao longo da vida. Vocês me inspiraram a perseguir um caminho em que eu pudesse buscar o que é certo, e, acima de tudo, justo para a comunidade. Não sei se algum dia serei capaz de retribuir devidamente, mas aqui exprimo, ou pelo menos tento, a minha profunda e eterna gratidão. À minha irmã Ana Clara, por todo o companheirismo, motivação e paciência. Obrigada por torcer pelo meu sucesso, da mesma forma que eu torço pelo seu, sempre.

Aos meus avós Teresinha e Heitor, Alvanea e João Bosco *(in memoriam*) e à minha bisavó Dulce, só tenho a agradecer pelo imenso carinho e a confiança de vocês ao longo da minha jornada. Vocês sempre me ensinaram muito.

À Ângela, agradeço por todo apoio e a fé que sempre depositou em mim. Minha prima Alexa, que sempre me incentivou, obrigada por sonhar comigo.

Aos meus fiéis amigos, Barbara Cruz, Izabella Rocha, Hélcio Neto e Paula Pacheco, estarei aqui por vocês sempre, agradeço por nossa amizade e desejo que ela se perpetue para a vida. Tenho certeza que sem vocês eu não aguentaria esses cinco anos, que por vezes pareceram intermináveis. De fato, vocês tornaram minha vida mais leve.

Ao meu namorado e grande amigo, Thales Teixeira, muito obrigada por todo companheirismo e amor, você fez com que eu mantivesse a calma e serenidade em momentos cruciais e sempre me proporcionou o apoio necessário para que eu seguisse adiante.

Aos membros da Clínica de Direitos Humanos do CESUPA, muito obrigada pelas experiências, aprendizados e por todos os momentos que compartilhamos, felizes, tristes ou desesperadores, vocês, em todos estes, me trouxeram felicidade, segurança e tranquilidade.

Ao meu orientador Prof. Dr. Dennis Verbicaro Soares obrigada por ter me auxiliado e por ter me permitido obter tantos conhecimentos em uma área que, até então, desconhecia.

Por fim, quero agradecer ao Centro Universitário do Estado do Pará por ter me propiciado as melhores bases para meu crescimento jurídico e pessoal. Em nome de todos os alunos desta instituição, eu não poderia deixar de agradecer especificamente a todos os professores que, tão gentilmente, compartilharam seus ensinamentos conosco e acreditaram no nosso sucesso como alunos e como pessoas. Vocês fazem a diferença na vida de cada um de nós e por isso, serei eternamente grata.

“Num tempo de engano universal dizer a verdade é um ato revolucionário”

(George Orwell)

RESUMO

Este trabalho teve por objetivo principal elucidar de que maneira ocorre a responsabilização civil decorrente do tratamento de dados pessoais nos contratos de consumo no comércio eletrônico, a partir da Lei Geral de Proteção de dados (LGPD), perpassando por questionamentos essenciais à compreensão da tutela jurídica dos dados pessoais, seu tratamento e as inúmeras violações de direitos aos titulares. Trata-se de uma monografia, oriunda da análise de dispositivos da Lei n.º 13.709/2018 e de uma pesquisa bibliográfica, desenvolvida por meio da leitura de livros, artigos científicos e notícias veiculadas em meios de comunicação em massa, utilizados para reiterar a relevância deste tema para a atualidade. Nessa pesquisa, investigou-se a situação do consumidor no comércio eletrônico, partindo da análise contextual das tecnologias da informação e seus impactos sociais, políticos e econômicos. Foram ilustradas, ainda, as principais formas de tratamento de dados, assim como os direitos fundamentais violados por essas práticas. Em seguida, retratou-se a questão do Direito à Privacidade e a vulnerabilidade situacional do consumidor em face das tecnologias de informação. Logo, buscou-se elucidar a imprescindibilidade da tutela jurídica da Proteção de Dados, pincelando de que forma se deu seu desenvolvimento, tornando possível apontar quais as principais fontes de influência para a construção de uma legislação específica nacional sobre esta seara. Posteriormente, foram averiguados os aspectos mais elementares da Lei Geral de Proteção de Dados, ressaltando seu caráter inovador. Finalmente, foi retratada a importância do instituto da responsabilidade civil para o comércio eletrônico, por meio da análise dos dispositivos da LGPD relativos à esta temática, de modo que restou demonstrada a necessária conjugação de fatores, tais como: atuação da Autoridade Nacional de Proteção de Dados (ANPD); a obediência as diversas fontes legislativas e principiológicas e a adequação cultural das empresas e agentes de tratamento para que seja dada efetividade ao recém- inaugurado regime geral de proteção de dados brasileiro.

Palavras-chave: Lei Geral de Proteção de Dados. Direito do Consumidor. *E-commerce.* Responsabilidade Civil.

ABSTRACT

The main purpose of this study was to elucidate the way in which civil liability derives from the processing of personal data in e-commerce's consumer contracts, based on the General Law on Data Protection (GLDP), leading to questions essential to the understanding of legal protection of personal data, its treatment and the numerous infringements of rights to the holders. This is a monograph, derived from the analysis of the provisions of Law no 13,709/ 2018 and a bibliographical research, developed through the reading of books, scientific articles and news published in mass media, used to reiterate the relevance of this topic to the present. In this research, the consumer's situation in electronic commerce was investigated, starting from the contextual analysis of information technologies and their social, political and economic impacts. The main forms of data processing, as well as the fundamental rights violated by these practices, were also illustrated. Then, the issue of the Right to Privacy and the situational vulnerability of the consumer opposite information technologies was portrayed. Therefore, it was sought to elucidate the indispensability of the legal protection of data, brushing how it was developed, making it possible to point out the main sources of influence for the construction of specific national legislation on this area. Subsequently, the most basic aspects of the General Data Protection Law were verified, highlighting its innovative character. Finally, the importance of the civil liability institute for e-commerce was shown, by means of the analysis of the GLPD provisions related to this subject, so that a necessary combination of factors has been demonstrated, such as: the National Authority for the Protection of Data (ANPD); the obedience to the diverse legislative and principles sources and the cultural adequacy of the companies and agents of treatment in order to give effectiveness to the recently inaugurated general regime of Brazilian data protection.

Keywords: General Law on Data Protection. Consumer Law. E-commerce. Civil Liability.

SUMÁRIO

1 INTRODUÇÃO

A partir da evolução dos meios de comunicação e da tecnologia, a informação adquiriu um novo patamar valorativo para a sociedade hodierna, sendo considerada como um novo tipo de insumo fomentador de relações sociais, políticas e econômicas da pós-modernidade. Contudo, apesar dos inúmeros benefícios trazidos pelos avanços tecnológicos à humanidade, deve-se ter em vista os impactos que o fluxo incessante de informações causa para as variadas esferas da vida dos indivíduos, pois o que se tem observado é uma interferência cada vez maior, e nem sempre consentida, na privacidade e na intimidade das pessoas.

Neste contexto, o advento da internet propiciou uma nova plataforma para relações jurídicas de todos os tipos, tendo em vista que permite o acesso rápido, garantindo comodidade e eficiência aos contratantes. Daí nota-se o crescimento exponencial de contratações eletrônicas de consumo no país, de tal forma que o direito não pôde se abster de tutelar estas relações para assegurar a proteção do consumidor e a garantia de seus direitos fundamentais. Vale ressaltar a situação de vulnerabilidade técnica, econômica e informacional do consumidor usuário de serviços disponibilizados na internet em face das pessoas jurídicas que nela atuam e que, muitas vezes, aproveitam-se de sua vulnerabilidade e de lacunas legislativas para agir de forma abusiva e prejudicial.

Assim, hoje, as práticas abusivas de tratamento de dados, dizem respeito ao mau uso destes, ou seja, a coleta indevida; a utilização para categorização e discriminação da pessoa; a publicidade individualizada; a manipulação; compra e venda destes dados. Tais práticas são apenas algumas das adotadas neste meio e ocorrem, majoritariamente, sem consentimento devido do titular, se utilizando de diversas técnicas para ludibriar o contratante.

Destarte, o Brasil promulgou a Lei Geral de Proteção de Dados, inaugurando um regime geral de proteção nacional, a fim de adaptar-se à realidade legislativa mundial, mas também para que as relações no âmbito virtual passem a ser pautadas por maior segurança no tratamento de dados pessoais, de modo a garantir sua continuidade como atividade econômica, além de assegurar a proteção direitos fundamentais, como o Direito à Privacidade e o Direito à Informação.

Não obstante, a eficiência do regime geral de Proteção de Dados dependerá da devida responsabilização daqueles que violem os referidos direitos e normas legais, a fim de reparar adequadamente os danos. Entretanto, isso não é tarefa fácil, uma vez que o ambiente virtual traz diversos entraves à adequada responsabilização, pois nele não existem fronteiras e impedimentos temporais. Isto posto, as informações podem ser processadas e copiadas

desmedidamente, somando ao fato da massificação e despersonalização inerentes dos contratos de *e-commerce*, o que dificulta ainda mais a identificação dos agentes de tratamento e fornecedores no comércio eletrônico. Tais características apenas corroboram a dificuldade em se mensurar a extensão dos danos causados e seus afetados, sendo este um dos maiores desafios apresentado aos legisladores, operadores do direito e sociedade civil.

Uma vez comprovada a complexidade e importância do tema, urge a necessidade de compreender melhor de que forma ocorre a responsabilização civil decorrente do tratamento de dados pessoais dos consumidores de serviços disponibilizados na internet. Por isso, na construção da presente monografia, utilizou-se de pesquisa bibliográfica de autores variados, tratando-se, primordialmente de obras sobre a Responsabilidade Civil, o Direito à Privacidade, Direito do Consumidor e a Proteção de Dados, tendo como foco as relações jurídicas de consumo no comércio eletrônico. Somado a isso, foi feita a leitura e análise de instrumentos legais, como o Marco Civil da Internet e a Lei Geral de Proteção de Dados (Lei n.º 13.709/2018), de forma mais aprofundada com relação aos dispositivos que dizem respeito ao tratamento de dados pessoais e a responsabilização dos agentes de tratamento.

Objetivando obter respostas a esse questionamento, foi primeiramente necessário investigar o contexto em que ocorrem os contratos de *e-commerce* e quais as características principais desses instrumentos que mais afetam a condição do consumidor, reforçando sua suscetibilidade às práticas abusivas no tratamento de dados. Ademais, foi essencial apresentar algumas das operações mais usuais de tratamento de dados realizadas atualmente, de modo demonstrar algumas das formas por meio das quais os usuários têm seus direitos violados.

Posteriormente, apontou-se a necessidade da atuação do direito na Proteção da Dados, com ênfase nas relações de consumo. Para isso, inicialmente, analisou-se a situação do Direito à Privacidade na sociedade da informação e a vulnerabilidade gerada ao consumidor a partir de seu contato crescente com as tecnologias da informação. Assim, fornecendo melhores bases para a compreensão do regime jurídico de proteção de dados dos usuários de internet, tanto no âmbito internacional quanto nacional, sendo referenciadas as principais influências legislativas para o desenvolvimento da Lei Geral de Proteção de Dados brasileira (Lei 13. 709/2018). Nessa linha, este trabalho buscou realizar uma análise objetiva dos aspectos basilares da recente Lei Geral de Proteção de Dados, para então partir para averiguação de seus elementos inovadores como a definição dos agentes de tratamento de dados e suas principais funções.

Por fim, considerou-se essencial discorrer acerca da responsabilidade civil no comércio eletrônico, realizando análise crítica das formas de responsabilização adotadas pela nova lei. Nesse sentido, foi necessário, também, elucidar os entraves no processo de criação da

Autoridade Nacional de Proteção de Dados, assim como, seu importante papel na efetividade do sistema de proteção de dados nacional, principalmente no que tange a responsabilização civil dos agentes de tratamento.

2 O CONSUMIDOR NO COMÉRCIO ELETRÔNICO

É imprescindível reconhecer que o desenvolvimento tecnológico teve grande impacto sob os seres humanos, especificamente sob a maneira como o ato de consumir é interpretado e valorizado. Segundo Soares e Verbicaro (2017), além de apenas fomentar o comércio de bens e serviços, atualmente, o consumo também representa uma importante ferramenta de inserção social, sendo simbólica para a própria existência dos indivíduos perante a sociedade.

Nota-se que o avanço da técnica nos meios de comunicação, permitiu maior alcance e também maior controle sobre o comportamento humano, tanto na esfera individual quanto social; a partir daí observamos o surgimento não espontâneo, mas na verdade imposto, de uma certa cultura, de forma a padronizar e inserir na sociedade determinados valores que beneficiam o tipo de consumo objetivado pela lógica capitalista vigente (SOARES; VERBICARO, 2017).

É esta indústria cultural que dita as regras comportamentais da sociedade e por isso é importante conhecê-la para também interpretar as relações consumeristas atuais:

> Nesse contexto, a técnica converte-se em psicotécnica, em artifícios de manipulação típicos da aparência fetichista das sociedades de massas. As pessoas transformam-se naquilo que o sistema, triturando-as, força-as a ser. Estão todos tão impregnados pelos esquemas da indústria cultural e sua exploração sistemática e programada de 'bens culturais' para fins comerciais, que o que se vê é uma tentativa de fazer de si mesmo uma vida que corresponda, *ipsis litteris*, ao modelo apresentado pelos seus *standards*, donde se concebe a espontaneidade e a liberdade individual no plano da mera abstração de pensamento. Eis o trunfo da publicidade e da manipulação da indústria cultural, cujo resultado é a mimese compulsiva dos consumidores às mercadorias culturais da sociedade industrial e de consumo e a naturalização da sua linhagem a ponto de criar um repertório de gestos padronizados e estigmatizados (SOARES; VERBICARO, 2017).

A industrialização e o consequente desenvolvimento da economia baseada em sistemas de produção em massa contribuíram para o surgimento de um novo modelo de contrato. Se antes o grande paradigma da teoria contratual era autonomia da vontade, tendo inclusive força de lei entre as partes, com o crescimento do consumo em massa e da abertura de novos mercados exigida para escoar tamanha produção outros fatores ganharam maior relevância, tais como a simplicidade, o dinamismo e a proteção da parte mais vulnerável da relação (CELLA; DONEDA, 2009).

Cella e Doneda (2009) ainda ponderam que, por outro lado, este novo contrato da era de produção em massa, deixa em segundo plano aspectos como negociações preliminares demoradas e minuciosas. A produção em massa acabou por gerar um contrato também

massificado, de moldes padronizados, nos quais não há espaço para particularidades e especificidades; neles não há tempo para discussão das cláusulas, apenas adere-se a elas na exata maneira como foram formatadas e por isso são classificados como contratos de adesão.

A partir da segunda metade do século XX, com a "rápida difusão das plataformas digitais e interativas como meio para realização de contratos" (CELLA; DONEDA, 2009), o comércio eletrônico passou a crescer exponencialmente, representando forte mudança no ambiente de consumo. Longe de se restringir apenas a contratações civis, empresariais e financeiras, os contratos de *e-commerce* que versam sobre relações consumeristas tornam-se a cada dia mais relevantes, de fato, percebe-se que este tipo de contrato é, hoje, uma das principais maneiras com que o consumidor se relaciona com os fornecedores e adquire bens e serviços desejados.

> Efetivamente, desde a década de 90, há um espaço novo de comércio com os consumidores que é a internet, as redes eletrônicas e de telecomunicação de massa. Trata-se do denominado 'comércio eletrônico', comércio entre fornecedores e consumidores realizado através de contratações a distância, que são conduzidas por meios eletrônicos (*e-mail* etc.), por internet (*online*) ou por meios de telecomunicação de massa (*telemarketing*, TV, TV a cabo etc.), sem a presença física simultânea dos dois contratantes no mesmo lugar (e sim a distância) (MARQUES, 2016).

Em muitos aspectos, a sociedade vive numa era digital, na qual a tecnologia não representa somente um aparato secundário na vida humana e sim parte integrante das relações diárias dos indivíduos, sendo muitas vezes indispensável. Nesse sentido, os avanços tecnológicos hoje permitem a criação de uma espécie de grande comunidade global, na qual é possível, por meio da internet, ter acesso simultâneo a informações, pessoas, bens e serviços espalhados pelo mundo (PINHEIRO, 2010).

Na mencionada comunidade global é constatada a transnacionalidade das relações de consumo contemporâneas. Os contratos de *e-commerce* costumam exceder o mero elemento internacional, como concebido tradicionalmente, e tornam-se transnacionais, da feita que o lugar efetivo da contratação passa a ser uma abstração e a nacionalidade das partes perde a sua importância (SCHREIBER, 2014).

> A internet suprimiu a referência física, geográfica, ao lugar da contratação, noção que era tão cara ao raciocínio do direito civil e do direito internacional privado. Um consumidor brasileiro, em viagem pela Europa, pode visitar o site de uma livraria de Nova Iorque, hospedado em um provedor da Califórnia, para adquirir um livro escrito por um autor francês, produzido por uma editora do Canadá, que lhe

> será expedido por um distribuidor situado no México ou na Argentina (SCHREIBER, 2014).

O atrativo desse tipo de relação contratual jaz no fato de que a internet é a plataforma mais eficaz para atender as exigências modernas de comodidade e agilidade, conectando as pessoas diretamente aos bens de consumo almejados sem necessidade de dispender muito tempo nesta busca. Este acesso direto, facilitado pela simplicidade de um "click", funciona como verdadeiro chamariz para uma extensa rede de consumidores, os quais passam a ter contato com uma infinita diversidade de informações, produtos e serviços sem precisar sair de casa.

Para fins organizacionais, podemos classificar os contratos eletrônicos quanto ao meio e a forma:

> a) Os contratos eletrônicos intersistêmicos seriam aqueles realizados entre sistemas de comunicação eletrônico com programação previamente estabelecida pelo fornecedor. São normalmente utilizadas em redes internas de comunicação dos fornecedores. b) Os contratos eletrônicos interpessoais presumem comunicação prévia entre as partes, como o ocorrido em chats (simultâneo) ou correios eletrônicos (não simultâneo) para que se realize a oferta do bem ou serviço a ser adquirido. c) Já os contratos interativos, os quais figuram como os mais populares dentro do e-commerce, se tratam daqueles em que o consumidor acessa o estabelecimento virtual pré-estabelecido do fornecedor (loja virtual), sem a possibilidade de negociação, mas apenas de aceitação interativa do produto ou serviço (ROSSI; SANTOS *apud* BORGES, 2018).

Apesar da classificação, observa-se que é característica inerente de todos os contratos de *e-commerce*, a utilização de um meio eletrônico pelo qual a contratação é realizada, de forma a não haver a necessidade de as partes encontrarem-se ou estarem presentes nos mesmo tempo e espaço. Tal distância, imposta entre as partes pelo meio, leva a uma 'desumanização do contrato', termo originário da doutrina italiana, que diz respeito à impessoalidade intrínseca destes instrumentos, da feita que, além da distância, os consumidores devem lidar com a massificação e generalização das cláusulas contratuais (MARQUES, 2016).

Analogamente ao entendimento de Cláudia Lima Marques, José Renato Cella e Danilo Doneda (2009) consideram que a falta de interação real entre os negociantes no contrato eletrônico realça ainda mais a assimetria entre partes que já era presente no comércio massificado tradicional, qual seja a definição unilateral dos termos contratuais. Isto reforça também o apelo pela proteção da parte que não tem a faculdade efetiva de negociar conforme suas contingências.

Outro fato que contribui para a sensação de despersonalização dos contratos eletrônicos é que no âmbito da internet, diferentemente do mundo real, não existem fronteiras físicas, aspecto que torna difícil definir materialmente quem são os fornecedores, uma vez que sua presença é meramente virtual e carecem de territorialidade, podendo ser qualquer sujeito e estar em qualquer parte de mundo (MARQUES,2016).

O mundo virtual rompe o entendimento tradicional de territorialidade, tornando-se um verdadeiro mundo *per se* em que a demarcação de territórios é difícil, se não impossível e onde as mais diversas culturas se relacionam constantemente e simultaneamente (PINHEIRO, 2010). Pelo exposto, esse aspecto pode tornar difícil a aferição, por parte do consumidor leigo, de como devem ser aplicados os efeitos daquela relação jurídica, quais os seus direitos dentro do contrato firmado e a qual ordenamento jurídico ou norma a relação deve se submeter.

Nessa seara, Schreiber (2014) alerta que a falta do elemento espaço-tempo nos contratos eletrônicos de consumo tem aproveitado mais extensamente aos fornecedores, os quais, atuando no ambiente virtual, frequentemente almejam se esquivar da aplicação de normas jurídicas que regulamentam as relações de consumo e ainda são capazes de reduzir os gastos inerentes ao processo econômico de disponibilização de bens e serviços. Em condições como estas, o direito deve impor resistência às conveniências do mercado, tomando sempre como norte o princípio da proteção mais efetiva do consumidor dentro destas relações.

Por estar exposto a riscos superiores, naturalmente em todas as suas relações contratuais, o consumidor enfrenta nos contratos de *e-commerce* ainda mais desafios:

> Tendo em vista a deterioração da noção de sujeito da relação contratual, o atual modelo de vinculação jurídica entre consumidor e fornecedor de aplicativos e *softwares* acentua a vulnerabilidade daquele, pois as cláusulas, que seguem o modelo de contratação padronizada mediante contrato de adesão (art.54,caput, e §§ 1.º a 4.º, CDC), não podem ser propostas ou flexibilizadas entre as partes, apenas unilateralmente pré-constituídas, devendo ser aceitas ou rechaçadas em bloco, razão pela qual a contratação eletrônica é também massificada. (VERBICARO; MARTINS, 2018)

As características próprias dos contratos de consumo eletrônicos, tais como sua inerente impessoalidade; massificação das cláusulas e a linguagem pouco acessível ao sujeito não versado em tecnologia, somadas a necessidades atuais de consumo cada vez mais vorazes, fazem insurgir a exigência ainda maior de proteção da parte mais vulnerável da relação: o consumidor.

As ações dos fornecedores atuantes no *e-commerce* também devem se pautar de maneira mais incisiva no resguardo do consumidor e seus direitos. O dever de informar serve,

justamente, ao propósito de amenizar a vulnerabilidade do consumidor, deixando-o mais consciente no que tange o teor das cláusulas do contrato, além de evitar vícios de consentimento. Impera lembrar que o meio virtual em que se dão essas contratações, não exime o fornecedor de agir em consonância com o princípio da boa-fé objetiva que rege as relações contratuais, na verdade, o meio virtual, por suas características típicas, ressalta ainda mais a necessidade de atitudes cuidadosas por parte dos fornecedores (VIAL, 2013).

> Através desse princípio é que as relações de consumo mudaram, assim os deveres principais da obrigação deixam de ser os únicos exigíveis, sendo também necessário o cumprimento de deveres laterais: *cuidado, previdência, segurança, cooperação, informação* (VIAL, 2013).

O princípio da confiança também permeia as relações contratuais de consumo, semelhantemente à boa-fé objetiva, pois versa sobre a crença das partes na conduta idônea e correta numa relação contratual. Esta confiança leva o consumidor a adotar certos comportamentos mesmo inserido em contingências sob as quais não possui domínio, podendo assumir riscos com base na esperança de que eles não se concretizarão (CARNEIRO DE FRADA *apud* MIRAGEM, 2016).

Sobre o princípio da confiança nos contratos de consumo, Bruno Miragem faz importante consideração:

> Com respeito às relações de consumo, a proteção da confiança é antes de tudo uma resposta à massificação das contratações e das práticas negociais de mercado. Uma das consequências desse fenômeno nas relações de consumo, já referimos, é a crescente despersonalização do contrato, fazendo com que os consumidores, sejam identificados pelos fornecedores, não mais pessoalmente, senão a partir de toda espécie de informação, como um número, uma senha ou determinados perfis de consumo, por exemplo (MIRAGEM, 2016).

Nesse contexto, "estes aderem sem conhecer as cláusulas, confiando nas empresas que as pré-elaboram e na proteção que, esperam, lhes seja dada por um direito mais social", conforme frisa Marques (2016), por isso, no momento em que a confiança depositada pelo consumidor é violada surge a possibilidade de responsabilização do fornecedor (MIRAGEM, 2016).

Ainda que a simplicidade, nos contratos eletrônicos de consumo, seja uma qualidade buscada pelos consumidores, esta mesma característica aprofunda a sua vulnerabilidade em relação ao fornecedor, tendo em vista que a maneira simplificada como o consentimento ocorre por este meio acaba por fazer com que o contratante concorde com cláusulas abusivas, as quais,

na maior parte das vezes, passam despercebidas, permitindo violações aos seus direitos. Aliado a isso, por ter natureza de adesão, a não aceitação das cláusulas do contrato impossibilita a utilização do serviço ou aquisição do bem, levando o consumidor, ávido à obter a satisfação de seus desejos e confiando plenamente na segurança daquela relação, a eximir-se de sequer ler o contrato e optar por consentir com seus termos, sem se dar conta de possíveis consequências negativas (VERBICARO; MARTINS, 2018).

Resta dizer que nem sempre o contratante terá o conhecimento qualificado o suficiente para discernir quais relações são vantajosas ou apresentam problemas para si e de que forma seus direitos são realmente amparados no meio virtual. Constatado o abismo técnico e econômico entre o usuário do serviço na internet e aquele que o fornece, somado a escassa responsabilização por práticas abusivas no comércio eletrônico, muitos fornecedores aproveitam-se para agir livremente, sujeitando o consumidor a riscos e prejuízos graves. Matérias como a proteção de dados pessoais, por exemplo, são constantemente alvo de violações nos contratos de *e-commerce*, especialmente em se tratando da utilização, armazenamento e até a venda de dados pessoais para usos desconhecidos de seus titulares e objetivos econômicos alheios a sua vontade.

2.1 Proteção de dados pessoais nos contratos de *e-commerce*

Os dados pessoais possuem, no comércio eletrônico, um papel de suma importância para consumidores e fornecedores, uma vez que seu fornecimento pelos usuários é indispensável na maioria das relações contatuais virtuais, seja para assinar um serviço, adquirir um produto ou cadastrar-se em uma rede social ou site. Desta maneira, "a importância da tutela jurídica dos dados pessoais reside no fato de que esses dados, assim como as demais informações contraídas, constituem uma representação virtual da pessoa perante a sociedade, constituindo verdadeira parcela de sua personalidade" (SOUZA, 2018).

Nesse sentido, Pinheiro (2010) ressalta que com a evolução dos meios de comunicações e da tecnologia, a informação passa a ganhar ainda maior relevância na mesma proporção em que seu alcance torna-se cada vez maior, sendo possível dizer que esta representa um novo tipo de moeda que move a sociedade contemporânea a tal ponto que transforma o direito à informação em fundamental para diversos ramos do direito. Portanto, num contexto em que as informações são tão valiosas, os dados pessoais dos consumidores representam grande trunfo para os fornecedores de bens e serviços no vasto comércio eletrônico.

Não obstante, Pires (2014) complementa que apesar dos inúmeros benefícios trazidos pelos avanços tecnológicos à humanidade, deve ser levado em consideração o crescimento da interferência na privacidade e na intimidade das pessoas.

> O tema da proteção do direito à privacidade do Homem em face do avanço tecnológico, principalmente com o advento da internet, desperta uma acalorada discussão. De um lado, o interesse dos Estados em controlar tudo e dos prestadores de serviços da sociedade da informação em obter dados dos usuários da Rede para suas campanhas publicitárias, do outro, o cidadão comum, cujos dados pessoais caem domínio público, que anseia uma livre navegação e a comunicação na internet, isenta de qualquer tipo de monitoramento (PIRES, 2014).

A realidade na *world wide web* é de que, não somente a definição de um domínio ou jurisdição aplicável ao território virtual é difícil, mas também a definição dos sujeitos que nela navegam, levando a crença de que a internet é um espaço de clandestinidade onde atos ilícitos podem ser cometidos em anonimato. Daí também nasce a importância da identificação dos sujeitos ao acessar aquele meio; não pode ser considerada uma solução, portanto, que proíba absolutamente que dados pessoais sejam captados na internet, mas sim que esse processo seja mais seguro para todas as partes, harmonizando o direito à privacidade e o direito à informação com os demais direitos fundamentais que possam entrar em conflito (PIRES, 2014).

Apesar de a definição técnica de dados pessoais não ser uniforme, considerando a definição legal mais recente adotada no Brasil: os dados pessoais podem ser definidos, conforme o art.5.º da Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709/2018), como informações que correspondem à um determinado titular, devendo ser pessoa natural identificada ou identificável. Ademais, existe uma modalidade específica de dados pessoais, também prevista na nova Lei, conhecida como dados pessoais sensíveis, os quais dizem respeito a informações de caráter personalíssimo como: raça, etnia, religião, opinião política, saúde, genética e até vida sexual (BRASIL,2018).

Um dado que qualifica um indivíduo como identificado trata-se de uma informação que pode ser associada diretamente com aquela pessoa, tal como nome, número de identificação pessoal, endereço etc. No caso de não haver nenhuma informação direta, serão esquadrinhadas outras informações, uma vez que outros dados podem ser processados em conjunto, no contexto da própria navegação do sujeito, permitindo sua associação com um indivíduo identificável (SARAIVA NETO; FENILI, 2018).

Hodiernamente, a plena identificação dos indivíduos no ambiente virtual é em muito facilitada por uma tecnologia conhecida como *Big Data*, a qual permite uma extensa análise e

correlação dos dados armazenados de cada pessoa, revelando informações pessoais em quantidade e velocidade antes inimagináveis (SOUSA, 2017).

Saraiva Neto e Fenili (2018) ressaltam que o *Big Data* não pode ser concebido apenas como tecnologia de processamento de dados, pois, na verdade, trata-se da massa de dados acumulada e composta de variados tipos de dados obtidos de diversas fontes, a qual pode ser armazenada e processada. Não obstante que o próprio recolhimento, armazenamento, análise, partilha, visualização desses dados e a privacidade de seus titulares, ainda representam grande desafio na lida com o *Big Data*, exatamente por conta da extensão do conjunto de dados envolvidos.

A variedade de dados passiveis de serem contidas no *Big Data* podem ser sumarizadas, consoante o entendimento de Dongpo, em três espécies diferentes, conforme a fonte:

> According to the sources of big data, big data can be divided into three categories: First, all kinds of data that come from people, people in the process of using the Internet, including video, pictures, text, etc.; second, from the machine, each The data generated by various types of computers in the course of operations is in the form of multimedia, databases, GPS, smart homes, documents, etc. The third is from objects. The data collected during the operation of various types of digital devices, such as digital signals acquired by the camera (DONGPO, 2018, tradução nossa).[1]

Na seara consumerista, a utilização do *Big Data* é benéfica para os fornecedores no comércio eletrônico na medida em que, se a sua capacidade analítica for aplicada corretamente, é possível, por exemplo, criar perfis comportamentais do consumidor, modificando e/ou direcionando as ofertas de bens e serviços e publicidade de acordo com o perfil desenvolvido. Os riscos à privacidade do consumidor assim demonstram-se pois, muitas vezes, o consumidor, como parte vulnerável, não terá conhecimento dessa prática ou não conhecerá seus reais efeitos, mas certamente será atingido por ela (SARAIVA NETO; FENILI, 2018).

2.2 Formas de tratamento de dados pessoais do consumidor no comércio eletrônico

O tratamento de dados pessoais pode se dar de diversas formas e servir a diversos propósitos. Notadamente, no âmbito do direito do consumidor, mais especificamente nos

[1] Conforme às fontes de *Big Data*, o *Big Data* pode ser dividido em três categorias: primeiramente, todos os tipos de dados que advém de pessoas, pessoas no processo de uso da internet, incluindo vídeos, imagens, textos, etc.; a segunda categoria vêm de máquinas, cada dado gerado por variados tipos de computadores no curso de operações está na forma de multimídia, banco de dados, GPS, *smart homes*, documentos, etc. A terceira vem de objetos. Os dados coletados durante operações de aparelhos digitais de vários tipos, tais como sinais digitais adquiridos por câmeras.

contratos de consumo eletrônicos, as operações de tratamento de dados guardam extrema importância, haja vista o valor designado às informações no cenário econômico e social atual.

A definição de tratamento de dados é geralmente descrita de maneira ampla, incluindo diversas operações, desde a coleta até a difusão de dados:

> Assim, o tratamento de tais dados constitui basicamente toda operação técnica com eles realizada, de modo informatizado ou não, com a finalidade de se refinar a informação, tornando-a mais valiosa ou útil. É feito pelos operadores, em nome dos controladores, a quem compete as decisões referentes. Tanto estes como aqueles podem ser pessoas físicas ou jurídicas, de direito público ou privado, sendo considerados agentes de tratamento. Aqui, os sujeitos detentores dos dados (a quem eles se referem) são chamados de usuários, vez que são os frequentadores de websites, os quais tem como editores aqueles que disponibilizam o conteúdo num espaço para que possa ser visualizado. Ainda nessa relação subjetiva, os provedores são as empresas que fornecem serviços de acesso e utilização de Internet pelos usuários (SOUZA, 2018).

No Brasil, a Lei Geral de Proteção de Dados, também de maneira abrangente, conceitua, em seu art.5.º, inciso X:

> Art. 5º Para os fins desta Lei, considera-se:
> [...]
> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL,2018).

Nos contratos de *e-commerce*, estas operações são facilitadas pela própria forma com que o contrato é celebrado; por terem natureza de adesão, sem o consentimento dado à todas as cláusulas formuladas unilateralmente pelo fornecedor, o consumidor é impedido de acessar o serviço ou adquirir o bem. Ademais, é notório que a maioria dos contratantes simplesmente dispensa a leitura do contrato.

O estudo " *The biggest lie on the internet: Ignoring the privacy policies and terms of service polices of social networking services"*, realizado por Obar e Oeldorf-Hirsch (2016, tradução nossa) constatou a gravidade desta problemática: 543 participantes foram submetidos à testes envolvendo a contratação de serviços disponibilizados na internet, nos quais, contidas na política de privacidade e termos de serviço, haviam cláusulas abusivas como a permissão para compartilhar dados pessoais dos usuários com terceiros. Surpreendentemente uma dessas

cláusulas permitia até que os filhos primogênitos dos usuários se tornassem propriedade da empresa fictícia. Os resultados neste teste revelaram que 399 dos 543 participantes, equivalente à 74%, ignoraram totalmente a leitura da política de privacidade; a explicação dessas pessoas foi bastante esclarecedora sobre o comportamento do consumidor na sociedade de informação, declarando que a conveniência e o fato de que a leitura dos contratos demandaria tempo foram alguns dos principais motivos para a rejeição de sua leitura por parte dos participantes.

Isto posto, o consumidor, mesmo dando seu consentimento expresso, está sujeito à violação de seus dados pessoais, seja por não ler devidamente o contrato ou por não entender as implicações de seu uso. Mais grave do que isso é o fato de que, com frequência, o simples fato de acessar um determinado domínio na internet exige a autorização, muitas vezes tácita e despercebida por parte do consumidor, de que certas informações pessoais sejam fornecidas.

O consentimento implícito é frequentemente adotado por provedores que tornam os termos e a política de privacidade disponíveis em *links* localizados nas margens da página ou do aplicativo, enquanto o *link* estiver acessível o uso do serviço sugere o consentimento implícito do usuário, tal prática é conhecida como *"browsewrap agreement"* (KUNZ *et al*, *apud* OBAR; OELDORF-HIRSCH, 2018, tradução nossa).

Sendo assim, os direitos do consumidor mais uma vez são colocados em perigo por práticas que se utilizam do suposto consentimento do contratante, tais como o *"clickwrap"* que questiona diretamente ao usuário sobre o seu acordo com os termos do contrato, fornecendo a política de privacidade na tela ou através de *links*. O consentimento, nesses casos, se dá por meio de um click pelo qual marca-se a opção de concordância com os termos e políticas de privacidade do contrato. Esta modalidade é mais similar ao consentimento informado do que outras práticas, porém não menos danosa, tendo em vista que a própria linguagem e estrutura dos contratos de *e-commerce* possuem aspectos que parecem, propositalmente, dificultar a leitura pelos consumidores (OBAR; OELDORF-HIRSCH, 2018, tradução nossa).

> The utilitarian approach of employing adhesion contracts when individuals are merely consuming products and services may seem reasonable; however, the shift toward social media prosumption, where the technology is driven by a mosaic of personally identifiable forms of user content generation (Obar & Wildman, 2015), suggests that the shoehorning of social media into traditional consumer regulatory silos via the adhesion contract may be problematic (OBAR; WILDIMAN *apud* OBAR; OELDORF-HIRSCH, 2018, tradução nossa)[2]

[2] A abordagem utilitária de empregar contratos de adesão quando os indivíduos estão meramente consumindo produtos e serviços pode parecer razoável; no entanto, a mudança para a suposição de mídia social, onde a tecnologia é impulsionada por um mosaico de formas pessoalmente identificáveis de

Embora aparentemente gratuitos, vários dos serviços e utilidades disponíveis em aplicativos móveis, na verdade tem nos dados pessoais fornecidos pelo usuário a sua fonte de lucro. Trata-se, portanto, de uma vantagem indireta obtida pelo fornecedor, pois a partir da coleta de dados do consumidor, obtém-se lucro na venda de relatórios sobre o uso de determinado aplicativo para empresas, as quais terão conhecimento de seu comportamento e preferências de consumo, tal prática é conhecida como *filtering* (VERBICARO; MARTINS, 2018).

Ademais, ainda conforme Verbicaro e Martins (2018), a partir da filtragem, troca e venda de dados pessoais do consumidor, as empresas podem também realizar o *profiling*, traçando perfis comportamentais de um determinado indivíduo e consequentemente tornando possível o direcionamento de publicidade específica designada para atender as demandas do consumidor, enquanto também as cria, de forma individualizada.

O monitoramento dos consumidores na internet é realizado principalmente pelos *cookies*, tecnologia que permite a análise da navegação de um usuário e que consiste em arquivos contendo informações básicas relacionadas às preferências dos usuários (SOUZA, 2018). Por meio da utilização de *cookies* a prática de *profiling* do consumidor é facilitada:

> Num contexto de publicidade comportamental (Online Behavioral Advertising - OBA), tais cookies irão permitir que as empresas publicitárias - e suas parceiras - reconheçam um usuário que retorna posteriormente ao website, o que permitirá, ao longo do tempo, a formação de um perfil consumidor. Levando-se em conta, ainda, as inúmeras possibilidades de processamento dos dados pessoais pelos meios automatizados, tão como a quase ilimitada capacidade de armazenamento, combinação e cruzamento de informações, é possível a formação de quadros de personalidade quase completos, aumentando exponencialmente as hipóteses de consulta e influência nos comportamentos dos indivíduos. Isso expõe ainda mais os usuários na Internet, reforçando a necessidade de estudo e regulamentação legislativa do tema (SOUZA, 2018).

Todas as formas supracitadas de utilização dos dados pessoais em contratos de *e-commerce* tem como princípio, o valor econômico e social atribuído aos dados pessoais do consumidor, os quais permitem aos fornecedores a obtenção de vantagens, na medida em que o conhecimento das preferências e comportamento do consumidor torna praticamente possível

---

geração de conteúdo do usuário (Obar & Wildman, 2015), sugere que o encaixe das mídias sociais em silos regulatórios tradicionais de consumo via contrato de adesão pode ser problemático.

prever qual serviço ou bem o usuário buscará em seguida e em decorrência disso poderá realizar apenas as ofertas que possuem mais chance de serem aceitas.

Nesse contexto, não é de surpreender que ao desejar um bem ou serviço, as pessoas se deparem com um anúncio em suas redes sociais que, magicamente, pareça ler nossas mentes, de fato não há nada de mágico nisso.

Importa reconhecer a hipervulnerabilidade, ou seja, a vulnerabilidade de maior gravidade e proporção massificada, na qual se encontra o consumidor nos contratos de *e-commerce*, partindo do princípio de que os dados e informações pessoais na internet podem ser infinitamente acessados e manipulados, de forma a urgir a necessidade de repensar a privacidade em novos parâmetros. Cautelas maiores, devem ser tomadas, por ambas as partes da relação, a fim de que sejam resguardados direitos fundamentais como o direito à privacidade dos usuários, desconhecedores da real dimensão da utilização de seus dados e os posteriores efeitos (VERBICARO; MARTINS, 2018).

A hipervulnerabilidade é encontrada no art.39, inciso IV do Código do Consumidor que prevê como "prática abusiva do fornecedor prevalecer-se da ignorância ou deficiência de julgamento do consumidor para impingir-lhe seus produtos e serviços" (VERBICARO; MARTINS, 2018).

Conclui-se que o tratamento de dados pessoais, em regra ocorre sorrateiramente, sem o consentimento qualificado do consumidor no que tange essas operações, as quais além de servirem primordialmente a interesses econômicos dos fornecedores também podem causar danos irreparáveis à privacidade dos contratantes. Daí torna-se imperativa a noção de que a tutela do direito do consumidor e da proteção de dados abarque possibilidades efetivas de responsabilização e reparação pelo tratamento indevido dos dados pessoais do consumidor.

3 A IMPRESCINDIBILIDADE DA TUTELA JURÍDICA PARA A PROTEÇÃO DE DADOS PESSOAIS DO CONSUMIDOR

3.1 Direito à privacidade na sociedade da informação

A personalidade humana pode ser subdividida em dois aspectos: a originalidade da pessoa humana, que diz respeito à sua individualidade, e a interdependência social e ambiental, que leva em consideração o homem no âmbito social de suas interações. Desta feita, ao relacionar-se com o meio social o homem adquire direitos e deveres (PIRES, 2014).

Segundo Pires (2014) a personalidade, do ponto de vista jurídico, deve ser compreendida como "a aptidão para ser titular de direitos e deveres perante determinada ordem jurídica, sendo o Estado o ente competente para reconhecer os direitos da personalidade", tal reconhecimento se dará por meio de normas, tanto constitucionais quanto infraconstitucionais e terá o fulcro de evitar abusos praticados por outros indivíduos ou pelo próprio Estado.

Os direitos da personalidade servem à proteção do homem, não na esfera patrimonial, mas, primordialmente, na sua essência. Conforme ensinam Pablo Stolze Gagliano e Rodolfo Pamplona Filho (2015): "conceituam-se os direitos da personalidade como aqueles que têm por objeto os atributos físicos e morais da pessoa em si e em suas projeções sociais".

Dada a sua relevância, o Direito à privacidade é amplamente tutelado no âmbito internacional, tendo lugar nas Organização Mundial das Nações Unidas em diversas convenções e tratados, incluindo a própria Declaração Universal dos Direitos Humanos, em seu artigo 12, de maneira que a privacidade é reconhecida mundialmente como um dos Direitos Humanos fundamentais. Consequentemente, inúmeros países possuem legislações internas que albergam a proteção à privacidade, dispensando a esse direito atenção especial (MENDONÇA, 2014).

Nestes termos, os Direitos da personalidade são também considerados Direitos Fundamentais no ordenamento jurídico brasileiro. Especificamente, o Direito à Privacidade possui previsão expressa no art.5.º, inciso X da Constituição Federal de 1988; assim sendo, nota-se que a constitucionalização do Direito à Privacidade é igualmente responsável pelo seu alto grau de relevância no ordenamento jurídico brasileiro:

> Deste modo, percebe-se que os direitos da personalidade se encontram constitucionalizados em um grau máximo, e declarados, do ponto de vista legal, como direitos fundamentais. Assim se obedece ao objetivo principal do legislador de garantir juridicamente os atributos inerentes

> à pessoa humana, defendendo a essência da sua personalidade, sendo imprescindível para o desenvolvimento integral da pessoa humana e, em todo caso, garantindo as suas qualidades mais peculiares e definidoras (DELGADO *apud* PIRES, 2014).

A partir da compreensão do que foi elucidado, fica demonstrada a importância do Direito à Privacidade. Sendo uma das espécies de direitos da personalidade, é, portanto, dotado de traços que lhe conferem alto grau de relevância em face de outros direitos, tais como: absolutos; gerais; extrapatrimoniais; indisponíveis; imprescritíveis; impenhoráveis e vitalícios.

Ressalta-se que o mencionado aspecto da indisponibilidade compreende ainda a irrenunciabilidade e a intransmissibilidade. A primeira pode ser compreendida como a impossibilidade de alterar o titular do direito, nem mesmo por sua própria vontade; já a irrenunciabilidade é compreendida como o impedimento em abdicar desses direitos, imperando o seu reconhecimento por razões de ordem pública. Não obstante, a intransmissibilidade versa sobre o fato de que não é permitido ao titular do direito cedê-lo a outro sujeito, como é possível, em regra, no caso de outros direitos privados (GAGLIANO; PAMPLONA FILHO, 2015).

Devido à sua natureza, o Direito à Privacidade deve ser tutelado por todos os ramos do direito, no entanto a sua proteção tem se tornado cada vez mais indispensável na seara do Direito do Consumidor, tendo em vista que o desenvolvimento tecnológico tem impactado diretamente na forma como as relações de consumo atuais são concretizadas, ou seja, pelo meio virtual, no qual não há noção de territorialidade ou temporalidade; onde é possível o anonimato e onde inúmeras informações circulam em fluxo constante.

Nesse cenário, o risco de violação à privacidade dos consumidores é ampliado por meio de práticas ilegais ou abusivas, utilizadas para monitorar, manipular e algumas vezes até discriminar, com base na captação e mau uso de informações pessoais dos consumidores no comércio eletrônico.

> Com o avanço tecnológico, os atentados à intimidade e à vida privada, inclusive por meio da rede mundial de computadores (Internet), tornaram-se muito comuns. Não raro, determinadas empresas obtêm dados pessoais do usuário (profissão, renda mensal, *hobbies*), com o propósito de ofertar os seus produtos, veiculando a sua publicidade por meio dos indesejáveis *spams*, técnica, em nosso entendimento, ofensiva à intimidade e à vida privada (GAGLIANO; PAMPLONA FILHO, 2015).

As tecnologias da informação existentes atualmente são interligadas por uma "linguagem comum", constituída pela geração da informação, seu armazenamento, processamento e transmissão. Incluem-se nessa categoria, a microeletrônica, a computação, as

telecomunicações e radiodifusão, a optoeletrônica, a engenharia genética e outros processos tecnológicos que têm como fundamento primordial o uso da informação como força motriz (CASTELLS *apud* PIRES, 2014).

Na medida em que ocorre o avanço das tecnologias supracitadas, os recursos informáticos passam a ter cada vez mais alcance, crescendo em acessibilidade, o que lhes garante um caráter universal. Desta feita, a intensa informatização da sociedade resultou também num rearranjo drástico de sua organização (MENDONÇA,2014).

A sociedade da informação, na qual vivemos hoje, é justamente o produto dessa reorganização, a partir da qual conhecimentos científicos, tecnológicos, dados e informações passam a substituir recursos naturais como principais fontes de riqueza e tornam-se agentes propulsores do progresso social, político e econômico da sociedade. Grande parte da economia está assentada na exploração econômica da informação, "resultando em uma substituição das variáveis centrais da atividade industrial - trabalho e capital - pelas variáveis centrais da sociedade pós-industrial – informação e conhecimento-, ou seja, bens imateriais" (GONÇALVES *apud* PIRES, 2014).

Com efeito, o desenvolvimento tecnológico gerou grandes impactos científicos, culturais, econômicos e sociais, por isso, a esfera privada dos indivíduos logo passou a ser também afetada pela profunda imersão nas novas tecnologias. Cabe frisar, que o tratamento de dados se apresenta como uma das áreas em que mais pesa a urgência de se definir critérios específicos e eficientes no que diz respeito à privacidade das pessoas.

Importa ser levado em consideração que o Direito à Privacidade, está intrinsecamente relacionado ao exercício de controle acerca do acesso a informações pessoais, quais sejam dados e opiniões relacionadas a um indivíduo específico. Nesta senda, o aprofundamento das reflexões a respeito das informações pessoais no ambiente virtual deu origem a expressão 'autodeterminação informativa', definida como: poder de determinação e controle da utilização de dados pessoais pertencentes à um indivíduo e exercida por este (MENDONÇA, 2014).

Outrossim, a doutrina e a jurisprudência já produziram conceitos variados de privacidade, nos quais fica clara a relação fundamental com a informação. Consoante o entendimento de Marcel Leonardi, podem ser resumidos em quatro categorias: "a) o direito de ser deixado só; b) o resguardo contra interferências alheias; c) o segredo ou sigilo; d) o controle sobre informações e dados pessoais" (LEONARDI *apud* MENDONÇA,2014).

O elo entre privacidade e proteção de dados, portanto, é demonstrado pela capacidade que os sujeitos ou instituições gozam para determinar quais informações de sua titularidade podem ser compartilhadas com terceiros, em que circunstâncias e para quais fins, isto é, o titular

das informações deve possuir a liberdade de escolher quais dados considera íntimos e confidenciais, controlando o acesso à estes mediante seu próprio consentimento.

De tal forma, nota-se que a tutela da privacidade serve de pressuposto para o exercício da liberdade, no sentido de que reforça a proteção contra interferências de estranhos que possam prejudicar o livre desenvolvimento da personalidade individual, sem contanto proibir a auto exposição das informações pessoais, desde que seja considerada a vontade do titular das mesmas (PIRES, 2014).

> Como visto, o objeto do direito à privacidade é definido pelo encontro entre o controle (autodeterminação individual) sobre informação com a esfera da vida privada. Nesse sentido, observa-se que o direito à privacidade amplia a noção do direito à autodeterminação informativa para além do tratamento de dados pessoais, abarcando também a proteção perante a intromissão na esfera pessoal e a tutela perante a difusão de afirmações pessoais e fatos verídicos. Em virtude disso, a concepção do direito à privacidade como garantia, em que não está em causa apenas a inviolabilidade física ou pessoal, mas também a autodeterminação informativa em relação à vida privada, faz com que no direito à privacidade se incorpore uma componente de liberdade (PINTO *apud* PIRES, 2014).

Apesar de a autodeterminação informativa possuir grande relevância à proteção de dados pessoais e ao exercício da privacidade, Danilo Doneda e Laura Schertel Mendes (2018) citam a estudiosa Helen Nissenbaun para defender que além de alterações no âmbito institucionais, deve existir uma nova interpretação acerca do conceito de privacidade *per se*, a ser concebido de forma mais complexa e ampla do que as definições anteriormente aplicadas, que tinham como foco apenas o controle do indivíduo sobre as suas informações pessoais ou a preservação da vida privada. Além desse aspecto, devemos nos ater também a importância econômica da informação na sociedade hodierna, fato que impede o controle totalitário da informação por parte de seu titular.

Segundo o entendimento de Helen Nissenbaun (2010, tradução nossa) as tecnologias da informação, abrem um leque de práticas nocivas à privacidade, tendo em vista permitem o monitoramento dos usuários, a formação banco de dados imensuráveis, entre outras operações informacionais, agravadas pela velocidade com que essa informação pode ser processada e distribuída pelo globo. Cada transformação tecnológica, é acompanhada por novas discussões e ameaças à privacidade, logo, ainda conforme a autora, é necessária a compreensão da privacidade inserida no contexto da sociedade informação.

Complementarmente, novos parâmetros devem ser erguidos com relação à privacidade para que ela possa ser efetivamente protegida e amparada mediante o contexto atual, inclusive com a criação de novos dispositivos legais mais atentos à realidade técnico-científica e social de hoje.

> These norms, which i call context-relatives informational norms, define and sustain essential activities and key relationships and interests, protect people and groups against harm, and balance distribution of power. Responsive to historical, cultural and even geographic contingencies, informational norms evolve over time in distinct patterns from society to society (NISSENBAUN, 2010).[3]

Isto é, partindo da concepção da privacidade em relação ao contexto atual, torna-se necessária a compatibilização dos ordenamentos jurídicos à nova realidade da privacidade, uma vez que tem se tornando cada vez mais ineficiente a sua tutela jurídica em face do crescimento e renovação das operações informacionais, como, por exemplo, o tratamento de dados pessoais.Com efeito, um fato que não deve nunca ser ignorado é a riqueza e rapidez com que as tecnologias mudam e avançam, criando relações e modificando as passadas, de tal forma que os legisladores sempre devem zelar para que não seja perdida utilidade social dos instrumentos legais.

Importa concluir que diante da sociedade da informação e do crescimento de práticas abusivas e inadequadas no que tange a utilização e apropriação das informações dos indivíduos, a proteção das informações pessoais deve se desenvolver para além de uma das faces da privacidade, fazendo urgir um estudo e uma tutela jurídica específicos, a fim de que a proteção efetiva dos dados pessoais dos cidadãos brasileiros possa ser alcançada (MENDONÇA, 2014).

3.1.1 A vulnerabilidade situacional do consumidor em face das tecnologias de informação

A atual sociedade pós-moderna possui como elementos fundacionais, primeiramente, a transformação radical das técnicas, tecnologia e, por fim, da forma de pensamento humano, fato que permitiu alterações sociais, econômicas e políticas. O entendimento dos mestres Erik Jayme e Cláudia Lima Marques é de que os elementos da sociedade pós-moderna que impactam frontalmente no mundo jurídico, são estes : a valorização dos direitos humanos; a elaboração

[3] Essas normas, que eu chamo de normas informativas relativas ao contexto, definem e sustentam atividades essenciais e relações e interesses fundamentais, protegem pessoas e grupos contra danos e equilibram a distribuição de poder. Em resposta às contingências históricas, culturais e até geográficas, as normas informacionais evoluem ao longo do tempo em padrões distintos de sociedade para a sociedade.

de normas para regular condutas pela exposição de seus objetivos, princípios e finalidades, conhecida como narração; a comunicação e o pluralismo, característica pungente na sociedade atual que se reflete multiplicidade de fontes legislativas possíveis para regular o mesmo fato jurídico (JAYME; MARQUES *apud* BORGES, 2018).

Para muitos, a pós-modernidade tem como um de seus maiores efeitos a descaracterização da individualidade dos sujeitos ensejando o aumento de sua dependência e vulnerabilidade perante a manipulação exercida pela indústria cultural, criadora de padrões e comportamentos exigidos pela sociedade hodierna. É certo que dentre os padrões impostos pela indústria cultural estão aqueles que dizem respeito ao consumo, fomentados pela racionalização da produção, padronização e crescimento da difusão das ofertas proporcionada pelas atuais tecnologias de informação (SOARES; VERBICARO, 2017).

De fato, a sociedade pós-moderna carrega grande dicotomia entre aspectos positivos e negativos. Se por um lado representa a desconstrução, indeterminação, ceticismo e deslegitimação das instituições, por outro lado também representa o encaminhamento da sociedade em rumo a uma nova racionalidade, pluralismo e relativismo cultural (BORGES, 2018).

Nesse contexto, o factível afastamento da realidade e a sua substituição pelo mundo virtual, decorrente da utilização cada vez maior das tecnologias de informação, propicia, dentre outras coisas, a neutralização do senso crítico do indivíduo, o qual passa a priorizar, primordialmente, a celeridade, ao invés da morosidade das relações jurídicas materiais. Em compensação, perde-se em segurança e aumenta-se a confiança, muitas vezes "cega", depositada pelo sujeito que almeja o atendimento ágil e eficiente de suas expectativas, tal qual uma máquina deve, em tese, fornecer (SOARES; VERBICARO, 2017).

Nessa linha, Marques (2004) afirma o surgimento de uma nova crise contratual, por conta da despersonalização intensa destes instrumentos, característica dos contratos de adesão em massa e, por conseguinte, dos contratos eletrônicos, constatando-se a "desumanização do contrato". Nas relações de consumo isso se torna ainda mais evidente, uma vez que, mediante a possibilidade de rápida e simples contratação, sem a leitura devida dos instrumentos, assina-se serviços e adquire-se produtos, gerando consequências muitas vezes imprevisíveis, pois com o consentimento não qualificado da parte, as empresas aproveitam-se para captar dados pessoais e realizar outras operações com a ignorância do consumidor.

A problemática em questão é tratada como uma forma de vulnerabilidade situacional do consumidor, caracterizada também pela excessiva confiança depositada pelo indivíduo no fornecedor, a qual é verificada insistentemente no âmbito das relações consumeristas de *e-*

commerce. De forma geral, a vulnerabilidade é reconhecida pelo Código de Defesa do Consumidor com o objetivo de garantir a harmonia nas relações de consumo e concretizar os princípios de proteção do consumidor, previstos pelo artigo 4.º do CDC. Com disposição expressa no artigo 4.º, inciso I do CDC, a vulnerabilidade é presumida em relação ao fornecedor como forma de resguardar o consumidor numa relação que é naturalmente desequilibrada (BORGES, 2018).

Cláudia Lima Marques (2006), elucida que a vulnerabilidade pode se manifestar de diversas formas, podendo ser técnica, jurídica, socioeconômica e informativa. Todavia, no contexto da sociedade atual, nomeada oportunamente de sociedade de informação, a vulnerabilidade informacional do consumidor, ganha novo destaque nas relações comerciais eletrônicas, isto porque o fornecedor é o maior detentor das informações e é aquele que as maneja, controla e manipula, muitas vezes em prejuízo do consumidor.

> O poder da informação sobre os produtos e serviços concentra-se nas mãos do fornecedor e, por conseguinte, é fator de desequilíbrio na relação estabelecida com o consumidor que busca por esses serviços e produtos, ainda mais ao adquiri-los fora do estabelecimento comercial, via Internet, em que a vulnerabilidade tende a se agravar, uma vez que, se de um lado há ampliação da oferta e da informação, por outro as características de distanciamento econômico e de conhecimento, presentes no mundo real, são acompanhadas das tecnológicas (LIMA *apud* SILVA; SANTOS, 2012).

A partir daí, desenvolve-se a noção de que a situação em que se encontram os consumidores hodiernamente, leia-se: a predominância das relações virtuais de consumo, detém características que implicam diretamente no agravamento de sua vulnerabilidade pré-existente, mais do que em contratos de consumo tradicionais. Logo, surge a necessidade de combater a dita vulnerabilidade situacional que aflige os contratantes.

Várias questões devem ser analisadas ao se tratar da vulnerabilidade do consumidor diante das tecnologias da informação, dentre as quais, se encontram as características inerentes dos contratos de adesão, os quais representam a maioria dos contratos eletrônicos disponíveis e nos fazem questionar até que ponto o consumidor tem a capacidade de fornecer seu consentimento qualificado e consciente no ambiente virtual. Sob estas premissas, Klee (2011) compreende que ao tratar de comércio eletrônico deve ser averiguada com mais afinco a manifestação de vontade do contratante, uma vez que na sociedade de consumo há uma massificação dos contratos e objetivação da vontade do aderente, a quem não é dada a faculdade

de participar da formação das cláusulas, causando a impressão de que o contrato foi celebrado sem a real consideração de sua vontade:

> [...] a utilização desmesurada dos contratos de adesão não leva em consideração a vontade da parte que se vê constrangida a aceitar as cláusulas contratuais, para ver seus interesses econômicos atendidos. Porque a manifestação da vontade não é totalmente livre, valoriza-se a sua declaração, tutelando-se a confiança despertada. Isto é, apesar de a manifestação de vontade do consumidor não ser totalmente livre, valoriza-se a sua declaração, tutelando-se a confiança despertada no cumprimento do contrato de adesão de uma forma qualificada (KLEE, 2011).

De todo modo, é válido dizer que os elementos os aspectos característicos dos contratos eletrônicos de consumo, tal qual ausência de presença física do fornecedor e a ausência de comprovação das informações por eles disponibilizadas devem compensadas pela prática de condutas de boa-fé, de maneira que o contrato venha a atender a confiança depositada pelo consumidor, a fim de resultar na realização de suas expectativas (BORGES, 2018). Por este motivo, entende-se que a boa-fé está interligada à confiança, da feita que o cumprimento regular das obrigações jurídicas permite a proteção da confiança justamente depositada (SILVA; SANTOS, 2012).

Ainda sobre esta seara, Marques (2004) defende que a boa-fé deve funcionar como uma forma de cooperação entre as partes, não se restringindo à um compromisso expresso, pois representa, na verdade, um "vínculo menos textual e mais leal" em relação as expectativas, de modo a inspirar confiança nas partes. Para reforçar a confiança nos contratos de *e-commerce* o fornecedor deve buscar atender os interesses, expectativas e direitos do consumidor, evitando causar danos e desvantagens excessivas, tendo em vista que tal cooperação permitirá o cumprimento das obrigações contratuais e, em consequência, trará benefícios a ambas as partes. Com efeito, o respeito ao dever de informar, que é dever anexo à boa-fé, é umas das formas mais eficientes de corresponder à confiança do consumidor e pode ser facilmente atingido pela simplificação e melhor apresentação das informações de qualidade nos contratos virtuais, dando destaque às informações e tornando-as claras, objetivas e acessíveis (SILVA; SANTOS, 2012).

Logo, é evidente que o combate à vulnerabilidade situacional do consumidor no comércio eletrônico perpassa pelo atendimento ao dever de boa-fé e seus deveres anexos, por meio dos quais os fornecedores refletirão uma realidade mais convergente à confiança, respeitando as necessidades e expectativas dos consumidores, de forma a garantir também o

necessário equilíbrio da relação jurídica. Por fim, não cabe olvidar que o direito também desempenha papel importante na recuperação da confiança do consumidor:

> apesar de não substituir a confiança que indivíduos depositam nas relações intersubjetivas, orienta quais expectativas possuem respaldo e resguarda a segurança de que estas serão atendidas; trata-se, portanto, de uma adaptação da confiança, pois, se por um lado há desconfiança sobre o contrato, há confiança no direito. No entanto, para que haja efetiva consolidação da confiança do consumidor no comércio eletrônico é necessária sua regulação e fiscalização constante (BORGES, 2018).

3.2 O regime jurídico de proteção do usuário na internet

Com base no que foi explanado ao longo do presente trabalho, se sabe que desenvolvimento da internet e das tecnologias da informação impulsionou o surgimento do comércio eletrônico, no qual relações de consumo, com o oferecimento de produtos e serviços, são firmadas por meios informáticos. Consequentemente, os fornecedores tiveram a oportunidade de ampliar sua capacidade econômica, atividades e negócios enquanto os consumidores também obtiveram o acesso à produtos e serviços facilitado, de forma a permitir sua aquisição mais rápida e simples.

Todavia, as características da desmaterialização; desterritorialização e despersonalização próprias dos contratos firmados no meio virtual, acabam por gerar efeitos diretos sobre o mundo jurídico, principalmente no Direito do Consumidor, uma vez que as mencionadas características reforçam ainda mais a vulnerabilidade do sujeito frente às ofertas dos fornecedores (MIRAGEM, 2016).

> Situações que envolvem questões relacionadas à saúde, educação, segurança, crédito, emprego, redes sociais, informações e até mesmo os rumos de um Estado Democrático de Direito dependem, cada vez mais, do uso massivo de dados pessoais e de processos totalmente automatizados de tomada de decisões que podem ter impactos diretos nas nossas vidas, inclusive nos sujeitando a práticas abusivas e discriminatórias (MONTEIRO, 2018).

A tutela jurídica que versa sobre a proteção do usuário de internet, consoante o ensinamento de Miragem (2016), deve ser concebida como de ordem pública, sendo indisponível pelas partes. Isto porque trata-se do exercício de direitos fundamentais à liberdade de expressão, à privacidade e à informação, além de prevalecerem as relações de consumo,

cabendo naturalmente à defesa destas normas como de ordem pública. Sendo assim, quaisquer tipos de abusos nestas relações jurídicas podem ser reconhecidos de ofício pelo magistrado, sem a necessidade de alegação pelas partes, portanto, priorizar-se-á a proteção do consumidor/usuário de internet.

Ademais, percebe-se que, ao longo dos anos, houve o fomento de práticas abusivas contra consumidores, realizadas em grande parte por agentes econômicos que se aproveitam da vaga e, ainda, pouco observada tutela jurídica sobre o assunto. Por isso, firma-se, neste trabalho, o entendimento de que é essencial a disciplina jurídica mais específica e melhor construída sobre esta problemática, tendo em vista a importância e natureza fundamental dos direitos envolvidos, tais como a privacidade e a informação, contanto, sem olvidar a importância do Código do Consumidor e de outras leis e princípios que vêm sido aplicados até então, devendo haver a complementariedade entre esses instrumentos.

3.2.1 Parâmetros jurídicos internacionais para o desenvolvimento da proteção de dados no Brasil

O surgimento da internet pode ser traçado ao período da Guerra Fria, no final dos anos 1960, no contexto do projeto *Advanced Research Projects Agency Network* (Arpanet) que era vinculado à *Defense Advanced Research Projects Agency* (Darpa), ambos financiados pelo governo estadunidense com o objetivo de construir uma forma de comunicação menos suscetível à ataques e falhas.

Entretanto, o que futuramente gerou impactos consideráveis à vida privada dos cidadãos comuns foi a criação da *world wide web*, no anos 1970. Encabeçada pelos pesquisadores Tim Berners-Lee e Robert Cailliau do *Conseil Européen pour la Recherche Nucléaire* (CERN), importância dessa tecnologia jaz no fato de que ela permite o compartilhamento de arquivos por intermédio de uma ferramenta de acesso conhecida como navegador (*browser*). Assim, a *world wide web*, com o passar do tempo, passou a ser confundida com a própria internet, no entanto ela é umas das várias ferramentas de acesso à internet, a qual revolucionou a dinâmica informacional na medida em que tornou possível a distribuição de informações e seu compartilhamento em computadores de maneira eficiente (FERREIRA; RODRIGUES, 2019).

A criação da "*web",* foi fator contribuinte para a existência da sociedade da informação em que estamos inseridos, porém, naquela época, os legisladores e operadores do direito passaram a conviver com novos dilemas. As alterações na sociedade, política e economia, decorrentes das recém-criadas tecnologias, fizeram despertar a necessidade da criação de um

direito que albergasse as novas relações jurídicas, entretanto o seu ritmo de transformação e a falta de "concretude" do meio virtual representam desafios à tutela jurídica que persistem até os dias atuais.

No que tange ao processo de regulamentação do Direito Digital, existiram discordâncias sobre qual enfoque seria dado pelo legislador. Consoante o ensinamento de Patrícia Peck Pinheiro (2010), a participação popular no processo regulamentador é indispensável, pois no Direito Digital a função legislativa é melhor aplicada quando o próprio interessado e participante das relações possui função ativa, já que este teria melhor conhecimento das brechas jurídicas e situações práticas vividas diariamente que não possuem proteção legal, consequentemente os interessados teriam maior noção de quais caminhos devem ser seguidos para o melhor atendimento de suas necessidades.

> Isso permite maior adequação do direito à realidade social, assim como maior dinâmica e flexibilidade para que ele possa perdurar no tempo e manter-se eficaz. Tal tendência de autorrregulamentação por meio do exercício da liberdade responsável e das práticas de mercado sem intervenção estatal é uma das soluções que mais atendem à necessidade de que o Direito Digital deve não apenas conhecer o fenômeno social para aplicar uma norma, mas ter uma dinâmica e uma flexibilidade que a sustentem na velocidade das mudanças da sociedade digital que sempre serão sentidas, primeiramente pela própria sociedade. (PINHEIRO, 2010)

Por outro lado é sabida diferença de poder, recursos e conhecimento jurídico que diferenciam um fornecedor de um consumidor, de forma a caracterizar sua vulnerabilidade e acarretando na exigência de que os Estados devam intervir para proteger estas relações e os indivíduos nela envolvidos, de maneira especial, a fim de diminuir os impactos negativos dessas diferenças sobre a parte menos poderosa da relação, tanto é que o ordenamento brasileiro apresenta diversos instrumentos com esta finalidade, tendo no próprio Código de Defesa do Consumidor um dos principais expoentes dessa concepção (MENDES, 2014).

Em âmbito regional a Comissão Interamericana de Direitos Humanos já começou a demonstrar a necessidade de preenchimento de lacunas normativas existente no Sistema Interamericano, tendo aprovado no dia 13 de dezembro de 2013 a Relatoria Especial para a Liberdade de Expressão e Internet (SALDANHA *et al.*, 2015). No entanto, o sistema regional ainda carece de disposições mais particulares sobre o assunto de proteção e tratamento de dados.

> Atualmente este é o principal documento do sistema interamericano sobre os princípios orientadores da liberdade de expressão na internet,

> dentre os quais figuram o acesso em igualdade de condições, o pluralismo, a não discriminação e a privacidade. Todos os princípios reconhecidos pela CIDH possuem estreita inter-relação, de modo que o desrespeito a qualquer deles compromete a efetivação dos demais. (SALDANHA *et al.*, 2015)

Em se tratando de regulamentação específica da matéria de proteção de dados pessoais, o direito internacional desenvolveu-se primeiro, por meio de convenções e tratados internacionais, os quais devem sua origem, em muito, às práticas costumeiras que regiam as relações virtuais antes de sua expansão mundial (SOUSA, 2017).

Internacionalmente, o direito que alberga a proteção dos indivíduos no meio virtual passou a ganhar ser destaque jurídico ainda nos anos 1970, pois logo se percebeu o risco à privacidade das pessoas e de seu monitoramento com a utilização daquelas tecnologias, as quais, paulatinamente, deixavam de servir apenas à propósitos militares e estatais e começavam a integrar à vida civil (FERREIRA; RODRIGUES,2019).

Naquele interregno, os Estados Unidos, editaram o *Privacy Act* em 1974, enquanto na Europa eram originadas leis voltadas para a proteção dos dados pessoais em países como Alemanha, França e Suécia. Já em 1981, o Conselho Europeu definiu dado pessoal como 'qualquer informação relativa a uma pessoa singular identificada ou susceptível de identificação' no âmbito da Convenção de Strasbourg. No ano de 1995, o Parlamento e Conselho Europeu editaram a Diretiva 95/46/CE, que dispunha em seu artigo 28, o dever de todos os Estados membros em formalizar e materializar uma entidade, a qual seria a autoridade competente para fiscalizar e aplicar as normas jurídicas sobre dados pessoais. Cerca de dois anos depois, a Diretiva 97/66/CE, regulamentou a privacidade na seara das telecomunicações (SILVA, 2019).

Nesse cenário, o chamado modelo europeu de proteção de dados, o qual tem como sustentação principal a Convenção do Conselho da Europa 108 de 1981, a Diretiva 46/95/CE e o Regulamento Geral de Proteção de Dados (Regulamento 2016/679), pode ser considerado como o sistema mais eficiente e centrado sobre a matéria retratada, dada a vasta regulamentação e constantes atualizações, tanto que guarda grande influência sobre os demais ordenamentos jurídicos do mundo (SILVA, 2019). Assim, Monteiro (2018) ressalta que o Regulamento Geral de Proteção de Dados da União Europeia, conhecido pela sigla inglesa GDPR, foi o responsável pela alteração da Diretiva Europeia de Proteção de Dados de 1995, resultando na atualização e adaptação da mesma às formas mais recentes de utilização massiva de dados pessoais, tais quais os modelos de negócios baseados nas tecnologias de *big data*, inteligência artificial, *cookies*, etc. Dentre outras disposições europeias, valem ser ressaltadas as infra citadas, dadas a sua

maior proximidade atinente as práticas abusivas no comércio eletrônico e o tratamento de dados pessoais:

> A Diretiva 2000/31/CE, de 8 junho de 2000, versou sobre o comércio eletrônico e, em 18 de dezembro de 2000, a Carta de Direitos Fundamentais da União Europeia, em seu art. 8º, referiu-se, de modo expresso, à "Protecção de dados pessoais", vindo, em seguida, a ser publicado o Regulamento (CE) 45/2001. Em 12 de julho de 2002, foi editada a Diretiva 2002/58/CE, denominada de "Diretiva Dados Pessoais nas Comunicações Eletrônicas", tratando da problemática atinente aos *spams* e *cookies*, ampliando a segurança quanto à confidencialidade. Já a Diretiva 2006/24/CE trouxe inovações sobre os direitos dos usuários do sistema informatizado quanto à retenção de seus dados e, em 2009, iniciou-se processo de atualização da legislação europeia por meio de consulta pública, advindo a Diretiva 2009/136, de 25 de novembro (SILVA, 2019).

Com efeito, as influências da regulamentação especial europeia podem ser encontradas no Brasil, mais recentemente, quando da feitura da Lei Geral de Proteção de Dados (Lei n.º 13.709/2018). Tal fato pode ser notado na exigência de parâmetros legais para o tratamento de dados; nos princípios gerais da Lei; nas previsões especiais para dados sensíveis e na criação de uma autoridade nacional executiva voltada para a sua aplicação. Além disso, a edição de regras específicas de responsabilidade do operador e controlador e a possibilidade de portabilidade de dados são hoje adotadas no Brasil, graças à evidente inspiração europeia. Não obstante, o ordenamento jurídico nacional abarcou outras referências internacionais advindas do direito norte-americano, tendo como exemplo a regra da notificação em caso de incidentes de segurança (art. 48 da Lei n.º 13.709/2018), prevista em leis estaduais dos Estados Unidos (DONEDA; MENDES, 2018).

Na própria américa latina, países vizinhos, como Chile, Argentina e Uruguai também desenvolveram legislações importantes para a ampliação da tutela jurídica dos dados pessoais. O crescimento da matéria em âmbito regional também levou o Brasil a subscrever-se, em 2003, a Declaração de Santa Cruz de La Sierra, na XIII Cumbre Ibero-Americana de Chefes de Estado e de Governo, na qual está previsto o direito fundamental das pessoas à privacidade, da mesma forma que dispõe a Declaração de Antígua, acarretando na criação da Rede Ibero-Americana de Proteção de Dados, aberta a todos os Estados da região (SILVA, 2019).

Outro fator a ser considerado que, simultaneamente, contribui para a escalada recente de regulamentação específica da matéria são as ocorrências de casos de grande repercussão envolvendo o tratamento e exposição indevidas de dados pessoais, gerando aumento da pressão social na adoção de medidas legislativas para a proteção dos indivíduos frente à grandes

empresas do ramo informacional e fornecedores do comércio eletrônico.

A renomada empresa Facebook forneceu informações pessoais de mais de 50 milhões de usuários para a empresa britânica Cambridge Analytica, que, por sua vez, utilizou as informações captadas com fulcro de manipulação política dos usuários da rede social (BBC, 2018). Já o site Ashley Madison, utilizado para encontros amorosos, foi atacado por hackers, levando à divulgação de dados pessoais de seus usuários, incluindo informações bancárias e fotos íntimas, de cerca de 37 milhões de perfis cadastrados no site, causando inúmeros danos (BBC,2018). Um dos casos mais recentes até esta data, envolve uma das maiores redes hoteleiras do mundo: a Marriott Internacional; estima-se que os dados de 500 milhões de clientes que se hospedaram nos hotéis da rede foram hackeados e levados a público (UOL, 2018).

Estas ocorrências demonstram ainda o despreparo, mesmo de grandes empresas e fornecedores de serviços, e a falta de medidas protetivas e preventivas em relação aos dados pessoais de usuários e consumidores. A extensão dos danos, tanto materiais quanto morais, causados às pessoas que tiveram dados pessoais revelados é difícil de auferir, pois quando essa divulgação se dá em meios virtuais as informações podem ser processadas e copiadas desmedidamente, além do fato de que não existem barreiras territoriais para a propagação desses dados, de tal forma que um hacker pode invadir o banco de dados de uma empresa localizada em qualquer parte do mundo, divulgando informações pessoais que também podem ter titulares de diversas nacionalidades (PINHEIRO, 2010). Assim, surge a clara necessidade de responsabilizar as empresas pelo mau uso e proteção desses dados pessoais de modo a reparar adequadamente os danos.

Todos as questões e instrumentos legais apresentados até então, contribuíram de alguma forma na adoção de uma legislação interna brasileira voltada para a privacidade no meio virtual e para a proteção de dados com fulcro de obter maior segurança aos usuários de internet. Logo, o Brasil, além de adotar convenções e tratados internacionais, passou também a construir, progressivamente, o amparo legislativo que abrigasse as relações no ciberespaço (MENDES, 2014). Daí é possível observar o surgimento de leis como a Lei de Acesso à Informação (Lei n.º 12.527/2011), o Marco Civil da Internet (Lei n.º 12.965/2014), entre outras.

Apesar da relevância que, merecidamente, dever ser dada às legislações supracitadas, não se pode olvidar que tais leis representam uma proteção setorial, abarcando a Proteção de Dados apenas em situações limitadas, de tal forma que é insuficiente a tutela dos direitos envolvidos. Nem mesmo o Código do Consumidor é capaz de satisfazer totalmente as necessidades consumeristas, no que tange esta matéria. Desta feita, era cediça a necessidade de

que houvesse previsões normativas capazes de expandir a proteção destes direitos à contextos mais diversificados, envolvendo o uso de dados pessoais, dentro e fora do ambiente virtual (MONTEIRO, 2018).

Anos de debates sobre a temática culminaram na constatação da insuficiência da tutela jurídica da Proteção de Dados nacional comparada a outros países e, especialmente, em face do contexto tecnológico, econômico e social da sociedade da informação, acarretando na compreensão de que é imprescindível uma legislação específica a ser aplicada à matéria.

Por sua vez, o Brasil acabou, sancionando, em 13 de agosto de 2018, a Lei Geral de Proteção de Dados, inspirada nas regulações europeias, americanas e nas leis nacionais já existentes, que conceitua e regula relações específicas na internet com o fulcro de, conforme seu artigo 1.º, amparar de maneira mais efetiva os direitos fundamentais de milhares de brasileiros vulneráveis a ter sua liberdade, privacidade e intimidade violadas. Ademais a Lei visa garantir o livre desenvolvimento da personalidade da pessoa natural, discorrendo sobre as mais diversas condutas e negócios possíveis, em se tratando de tratamento de dados pessoais com fins de exploração econômica e empresarial, assim como versa sobre a necessária responsabilização dos agentes que violem os direitos dos indivíduos (FRAZÃO, 2018).

Seguindo o mesmo raciocínio, Monteiro (2018) conclui que a promulgação da LGPD (Lei 13.709/2018) é de suma importância, pois ela modifica um sistema formado exclusivamente de leis esparsas, dotado de proteção setorial, para um sistema de proteção geral, que alberga o tratamento de dados pessoais, independente do setor, mercado e contexto.

Mediante a análise realizada, é válido dizer que a construção da legislação pátria reflete a convergência internacional, no sentido de que tem havido uma concordância mundial em relação à princípios básicos de proteção de dados. O autor Colin Bennett, teorizou que essa convergência se trata de um fenômeno internacional que ocorre informalmente, por meio do qual as legislações nacionais dos países acabam tornando-se cada vez mais semelhantes no conteúdo e na forma, atingindo patamar que excede até mesmo a realidade nacional. Por conta disso, é perceptível a identificação, ao longo da evolução normativa dos diversos Estados, de um padrão internacional de princípios de Proteção de Dados. Assim, as variadas influências estrangeiras que resultaram na Lei Geral de Proteção de Dados do Brasil são visíveis, entretanto, ainda que tenha como base o modelo europeu de proteção de dados, a supracitada Lei está conectada com a legislação e cultura jurídica brasileira, visto que ela inclui e complementa noções e dispositivos presentes nas leis já existentes no ordenamento jurídico nacional (DONEDA; MENDES, 2018).

Nessa linha, solução que congrega melhor a melhor aplicação da lei pátria deve ter

como corolário as suas múltiplas fontes influenciadoras. Tal pluralidade, deve ser sempre utilizada a favor do consumidor, aplicando-se harmônica e conjuntamente as mais variadas normas para criar um ‘diálogo das fontes’, conforme ensina o ilustre doutrinador Erik Jayme (MARQUES, 2016).

> Em resumo, hoje, na pluralidade de leis pós-modernas com seus campos de aplicação convergentes e flexíveis (envolvendo interesses- e direitos- coletivos, difusos, individuais homogêneos ou meramente individuais), a uma mesma relação jurídica de consumo podem ser aplicadas muitas leis, em colaboração, em diálogo, se afastando ou se unindo, caso a caso, com seus campos de aplicação coincidentes, em diferentes soluções tópicas para cada caso (MARQUES, 2016).

Destarte, as variadas fontes do tema da proteção de dados carregam o pressuposto de que é indispensável a sua tutela jurídica para a proteção dos cidadãos, principalmente dos consumidores, como categoria ainda mais vulnerável, mas também da sociedade como um todo, uma vez que inserida em um mundo, no qual os dados pessoais detém tanta importância dentro e fora do meio virtual. Por esta razão, a busca pelo tratamento responsável e legal dos dados pessoais, garante a proteção dos titulares destes dados e o exercício de seus direitos fundamentais, mas também resguarda a continuidade das atividades econômicas modernas. Deste modo, o sistema normativo de Proteção de Dados estabelece procedimentos, direitos e princípios com intuito de controlar o processamento de dados, ao mesmo tempo, em que empodera o cidadão para que disponha da capacidade de controle destes dados (DONEDA; MENDES, 2018).

3.2.2 A proteção de dados pessoais no ordenamento jurídico brasileiro

Nacionalmente, a desenvolvimento da internet se deu relativamente mais tarde do que nos países desenvolvidos, tendo iniciado no final da década de 80, enquanto sua popularização se deu, de fato, na década de 90, devido à iniciativa do então Ministério da Ciência e Tecnologia, com o objetivo de ampliar o acesso à rede à população brasileira como um todo, pois, até o momento, era aproveitado majoritariamente por instituições de pesquisa e universidades. A distribuição passou a ser executada somente pela Embratel e posteriormente por novos provedores de conexão que começaram a ofertar o serviço. (SANTOS; DUARTE, 2018).

Os reflexos do desenvolvimento informacional no país, a partir da crescente utilização e produção das tecnologias de informação no território nacional, logo inseriram o Brasil na *data driven economy,* economia baseada em dados, na qual lucra-se com a utilização das

informações dos indivíduos, cuja coleta, armazenamento e processamento são facilitados pelo meio virtual em que são disseminadas (OLIVEIRA, 2018). Consequentemente, imperava a necessidade de regular e fiscalizar aquele meio, de forma a adaptar o ordenamento jurídico brasileiro à nova realidade. De início, o Código Civil de 2002 disciplinava de forma genérica as novas relações jurídicas oriundas da evolução tecnológica, entretanto, desde àquela época, já era reconhecida a importância de criação de uma legislação realmente capaz de atender às peculiaridades do mundo virtual (SANTOS; DUARTE, 2018).

Partindo dessa premissa, o Brasil iniciou o desenvolvimento de legislações e dispositivos legais com aplicação voltada para as relações jurídicas na internet, perpassando pela proteção de dados pessoais, tais como o art.43 do Código de Defesa do Consumidor Código de Defesa do Consumidor, que versa sobre direito à informação e banco de dados; o art.4.º,VII do Decreto 7.962 de 2013 (LGL\2013\2685) (Comércio Eletrônico) e o Marco Civil da Internet (PINHEIRO, 2019).

Dentre outras legislações e tentativas legislativas, frisa-se a Lei n.º 12.695/2014, como umas das mais relevantes para fins de análise do crescimento da proteção de dados no país. A mesma é conhecida popularmente como Marco Civil da Internet e sua construção dependeu de um longo processo que envolveu consultas ao público em geral e à especialistas no assunto. No que tange seu conteúdo, cabe ser destacados o advento de preceitos como respeito à liberdade de expressão, o direito ao sigilo das informações, a responsabilidade civil, a neutralidade da rede, entre outros elementos que adquiriram previsão específica para o meio virtual.

Desta feita, o Marco Civil da Internet, possuiu como finalidade principal, prevista em seu art.1.º, de estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil, além determinar diretrizes de atuação para os entes federativos sobre a matéria (BRASIL, 2014). Apesar de ter representado certos avanços na proteção dos direitos individuais, num ambiente que por muito tempo foi considerado como excluso à legalidade, o Marco Civil da Internet trata apenas de forma superficial sobre a proteção de dados, pois tem como objeto legal a regulação geral do meio virtual, o que certamente não é capaz de abranger a real extensão das operações com dados pessoais para além da internet e nem a importância econômica e social atribuídas às informações pessoais e ao tratamento de dados como um todo (OLIVEIRA, 2018). Pelo mesmo motivo, pode ser afirmado que não há qualquer conflito entre o Marco Civil da Internet e a Lei Geral de Proteção de Dados, na verdade, há uma relação de complementariedade entre estes instrumentos, uma vez que a LGPD possui caráter de especialidade no que tange o tratamento de dados:

> A relação de especialidade entre lei nem sempre é clara, como podemos

> verificar na própria análise entre MCI e LGPD. É certo que ambas regulam o tratamento de dados, porém, enquanto a primeira não cumpre apenas esse papel, a segunda sim, pois seu fim específico é estabelecer parâmetros de proteção de dados pessoais em qualquer tipo de relação jurídica, independentemente da utilização da Internet (OLIVEIRA, 2018, p.6).

Os direitos previstos nos art. 7.º e art. 11 da Lei n.º 12.965/2014, são, ainda hoje, relevantes e essenciais, porém, refletem apenas o caráter genérico das informações, isto é, o direito ao sigilo, à autodeterminação informativa, exclusão definitiva de dados pessoais da internet, a necessidade de consentimento expresso para coleta de dados etc. Com efeito, nos anos que se seguiram à implementação da referida lei, persistiram lacunas que necessitavam de urgente regulação; devido à grandiosidade das operações envolvendo dados pessoais e os agentes econômicos nelas envolvidos, os danos causados aos usuários tornaram-se cada vez mais comuns e passaram a ganhar mais repercussão internacional.

Diante disso, no ano de 2018, o Brasil passou a integrar o grupo de países dotados de lei gerais voltadas particularmente para a Proteção de Dados, por meio da implementação da Lei n.º 13.709, de 14 de agosto de 2018, nomeada Lei Geral de Proteção de Dados (LGPD). O fator impulsionador e objetivo primordial de sua sanção foi a urgência de atualização dos mecanismos regulatórios nacionais em face do desenvolvimento e expansão tecnológica e o consequente crescimento do armazenamento, coleta, transmissão e processamento de dados, operações que se incluem na categoria genérica de tratamento de dados (PINHEIRO, 2019).

Desta feita, a LGPD inaugura o tão aguardado regime geral de proteção de dados pessoais, complementando o regime jurídico brasileiro de proteção dos usuários de internet ao juntar-se com o Marco Civil da Internet, a Lei de Acesso à Informação, o Código de Defesa do Consumidor, entre outras legislações, modernizando o tratamento da informação no Brasil. Em conjunto, estes instrumentos buscam fornecer o aporte das relações no âmbito virtual para que sejam pautadas por um maior respeito à garantias e direitos dos cidadãos, consequentemente por uma proteção mais efetiva aos direitos fundamentais, enquanto permite o desenvolvimento da economia da informação baseada na confiança, valor e segurança (DONEDA; MENDES, 2018).

3.3 Noções fundamentais da Lei Geral de Proteção de Dados (LGPD)

Para fins explicativos, a análise do referido instrumento legal se pautará na checagem de seus elementos basilares. Para isto, o presente tópico será subdividido em três partes: i) a

aplicabilidade da lei; ii) hipóteses autorizativas de tratamento de dados; iii) princípios do tratamento de dados.

3.3.1 A aplicabilidade da Lei. 13.709/2018

A unidade e generalidade da aplicação são características essenciais no âmbito de aplicação material de uma lei geral (DONEDA; MENDES, 2018). Na Lei n.º 13. 709/2018 o seu alcance pode ser encontrado nos artigos 3.º e 4.º da LGPD, enquanto o art.1.º estabelece objetivamente a matéria a ser tratada pela lei e seus principais objetivos, incluindo a previsão expressa de que a aplicação se dará aos dados pessoais também contidos em meios virtuais. Ecoando as palavras descritas no primeiro dispositivo da Lei, o art.3.º reforça que a LGPD deve ser aplicada à qualquer operação de tratamento de dados, feita por pessoa natural ou pessoa jurídica de direito público ou privado, independente do meio utilizado para tal, do país de sua sede ou do país onde os dados se encontrem.

Tais artigos, tem como pressuposto a notória falta de demarcações territoriais e fronteiras no ambiente virtual, assim como a internacionalização das relações jurídicas propiciadas pelas tecnologias de informação e refletem o entendimento já consolidado previamente em legislações brasileiras voltadas à regulação da internet, tal como o Marco Civil da Internet, que já continha disposição similar de que deve haver a proteção do cidadão brasileiro quando são parte de relações com agentes estrangeiros ou quando sejam alvo de suas operações (SANTOS; DUARTE, 2018). Neste ensejo, os incisos do art.3º discorrem mais detalhadamente sobre os elementos nacionais que permitirão a aplicação da LGPD, inclusive a hipótese de a operação ter sido efetuada por empresa estrangeira, com sede fora do país, bastando que o titular dos dados seja brasileiro.

O art.4.º, por sua vez, ilustra as situações em que não deve haver a aplicação da LGPD, isto geralmente será possível quando tais situações possuírem amparo em outros direitos fundamentais como, por exemplo, o direito à liberdade de informação. Dá-se ênfase à hipótese prevista no inciso I, a qual prevê que não pode ser aplicada a lei: quando o tratamento de dados pessoais realizado por pessoa natural possua fim exclusivamente particular e não econômico. Diante disso, se conclui que a preocupação primordial da Lei n.º 13.709/2018 é o amparo dos dados pessoais que venham a integrar relações com ganhos econômicos, as quais, em regra, representam os maiores riscos ao titular, tais como as relações de consumo.

As previsões acima retratam a generalidade da aplicação da lei no que tange as diversas formas de tratamento de dados e aos diversos sujeitos albergados por esta, além de que

permitem a unidade na proteção dos cidadãos brasileiros, reunindo num só instrumento legal os mais diversos direitos e deveres relacionados à matéria.

3.3.2 As hipóteses autorizativas de tratamento de dados

Outro elemento fundamental da Lei são as hipóteses autorizativas de tratamento de dados, as quais podem ser relacionadas diretamente com certos princípios fundamentais que também dizem respeito às relações de consumo. Nesta celeuma, cabe ao fornecedor, que executar o tratamento de dados do consumidor usuário, agir conforme à boa-fé, respeitando os demais princípios da transparência, confiança e, principalmente, da informação (GRANATO; COSTA, 2017).

Com base nisso, um dos pilares da LGPD é que o tratamento de dados não poderá ocorrer sem autorização, sendo esta a condição para a sua legitimidade. Isto posto, o tratamento será legítimo ao se incluir em uma das hipóteses previstas no art.7.º ou art.23 da referida lei e poderá se dar por meio de dois mecanismos autorizativos: consentimento do próprio titular dos dados ou por previsão normativa do tratamento (DONEDA; MENDES, 2018).

Ao estabelecer, de maneira expressa, o consentimento como primeiro requisito para o tratamento de dados legítimo, a LGPD reafirma o compromisso primordial de proteger amplamente o titular dos dados, isto porque a exigência do aceite significa considerar a existência de direitos e liberdades individuais para resguardar o indivíduo contra possíveis discriminações e prejuízos à sua dignidade (PINHEIRO, 2019).

> Art. 7º
> O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> [...] (BRASIL, 2018).

Nesse contexto, para que haja a validade do consentimento, o art.5.º, inciso XII, exige que este seja livre, inequívoco e informado, devendo ser considerado, ainda, que o consentimento se dará para o tratamento com uma finalidade previamente determinada, sendo esta, conhecida e aceita pelo titular. Ademais, o art.8.º, § 4.º e art.9.º, § 1.º da LGPD determinam que o consentimento genérico ou realizado a partir de informações abusivas ou enganosas será nulo. Merece destaque ainda a previsão da faculdade do titular de revogar o consentimento a qualquer tempo, fato que deverá ocorrer por meio de procedimento facilitado e gratuito, conforme o art.8º, § 5.º da supracitada lei. Estes artigos possuem o evidente objetivo de salvaguardar a privacidade e, mais especificamente, a autodeterminação informativa.

Além disso, o art.8.º, §2.º da LGPD ainda prevê que, nos casos de tratamento de dados entre particulares, basta a simples oposição para fazer óbice às operações, todavia em situações que envolvam o poder público (hipótese que independe da autorização do particular para a obtenção de dados), a oposição deverá se dar em conjunto com uma motivação (RODRIGUES; FERREIRA, 2019).

No que diz respeito aos dados sensíveis, conceituados pelo art.5.º, II da LGPD, o art. 11, I, da lei dispõe que, o consentimento deverá ser fornecido de forma ainda mais específica e destacada, isso se dá, evidentemente, pelo fato de esses dados possuírem natureza personalíssima extremamente relevante, tais como, informações sobre genética, saúde, opinião política, etc. Isto é, enquanto o consentimento para tratamento de dados deve ser livre, inequívoco e informado, o tratamento de dados sensíveis ocorrerá mediante consentimento livre, inequívoco, informado, específico e destacado (SANTOS; TALIBA, 2018).

Outrossim, tanto os dados sensíveis quanto os dados não sensíveis poderão ser tratados sem a necessidade de autorização expressa do titular, todavia, isso se dará apenas em situações descritas pela própria lei, tais como as previstas nos art.7.º , a partir do inciso II e art.11, a partir do inciso II da LGPD (MULHOLLAND, 2018).

Pelo exposto, consonante entendimento análogo de Bruno Miragem em relação ao Marco Civil, a Lei Geral de Proteção de Dados, foi capaz, de forma ainda mais aprimorada que sua predecessora, de estabelecer um procedimento específico para o tratamento de dados pessoais na internet, firmando um arcabouço de hipóteses legais para a ocorrência dessas operações, com o objetivo de resguardar a privacidade e o consentimento qualificado do consumidor usuário, de maneira a evitar vícios no negócio e outros prejuízos (MIRAGEM, 2016).

3.3.3 Princípios do tratamento de dados

A partir de uma leitura inicial da Lei Geral de Proteção de Dados, nota-se rapidamente o esforço dos legisladores em reiterar preceitos fundamentais do ordenamento jurídico brasileiro, de maneira que dedicaram boa parte do texto legal para reafirmar e estabelecer princípios, muitos dos quais já possuíam previsão legal ou mesmo constitucional.

A intenção é reforçar a ideia de que o meio virtual não pode e não deve ser tratado como cenário apartado da realidade jurídica nacional, realçando o pertencimento das relações abarcadas pela Lei à uma ordem sistêmica maior e, assim, resguardando sua unidade. Ainda conforme Danilo Doneda e Laura Schertel Mendes (2018), colocar os princípios em voga também leva em conta a recenticidade da matéria albergada pela lei e a necessidade em firmar

os limites para os seus princípios fundamentais, os quais, por si só, já apresentam forte carga substancial.

Nesta seara, Oliveira (2018) compreende que a LGPD teria criado princípios específicos ao tratamento de dados pessoas com a intenção de elevar o novo instrumento legal a um patamar referencial para a elaboração de legislações futuras, assim como para fins interpretativos de outras normas que venham a tratar de tratamento de dados.

Desde logo, a Lei n.º 13.709/2018 firma como objetivos, contidos no art. 1.º, o amparo à direitos fundamentais dos cidadãos brasileiros, onde cita-se a liberdade e a privacidade, além do livre desenvolvimento da personalidade da pessoa natural (FRAZÃO,2018). Sob tais premissas, a LGPD, no seu art.2º, apresenta os fundamentos para proteção de dados pessoais; em meio a estes são encontrados princípios caros à ordem constitucional, sem os quais seria impossível sequer estabelecer um regime jurídico de proteção de dados, exemplarmente cita-se o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão; a defesa do consumidor; etc. (BRASIL,2018).

Como se vê, a defesa do consumidor é deliberadamente expressa pelo legislador (art.2º, inciso VI, LGPD) como fundamento para proteção de dados. Esta escolha é bastante inteligente, levando em consideração o crescimento incessante das relações de consumo no comércio eletrônico, onde ocorre a maior parte do tratamento de dados. Assim sendo, hoje já é possível dizer que a maioria dos negócios onerosos na internet possuem relação com a aquisição de bens e serviços, vem daí a necessidade de proteção expressa do consumidor como usuário majoritário e, ao mesmo tempo, mais vulnerável do meio virtual.

Com efeito, sabe-se que mesmo antes do advento de legislação específica para a proteção do consumidor usuário de internet, o Código de Defesa do Consumidor já era aplicado de forma plena aos contratos de consumo no *e-commerce.* Isto por que, conforme Klee (2011) "a internet não é uma nova fonte de obrigações, nem cria novo tipo contratual, mas é um outro meio através do qual o consumidor pode se relacionar com os fornecedores de produtos e serviços". Portanto, é perceptível a estreita relação entre os princípios do Direito do Consumidor e os fundamentos utilizados pela Lei Geral de Proteção de Dados para reger a proteção e o tratamento de dados de pessoas naturais no ambiente virtual.

Outrossim, a Lei, por meio do estabelecimento de princípios e direitos do titular, almeja estruturar instrumentos que garantam ao indivíduo, essencialmente, o controle sob seus próprios dados em face de terceiros. Para isto, a LGPD lida com o tratamento de dados sob a ótica de contratos onerosos, atribuindo à estas operações uma série de princípios a serem observados a fim de conceder-lhes a devida legalidade.

Os princípios do tratamento de dados podem ser encontrados expressos no art.6.º da Lei Geral de Proteção de Dados, mesmo assim outros poderão ser auferidos através de uma leitura sistêmica. O referido dispositivo carrega dez incisos com princípios variados, todavia ressaltam-se os seguintes:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> [...]
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (BRASIL,2018).

Observando o caput do artigo em epígrafe, conclui-se que opção da lei em utilizar princípios específicos como norte para o tratamento de dados acaba por estabelecer um "procedimento especial" para a legalidade dessas operações (MIRAGEM, 2016). Isso ocorrerá, da feita que cada um dos princípios ilustrados se porta como requisito para celebração do tratamento de dados e, portanto, servirão como base para a configuração ou não de sua conformidade legal.

Nesta celeuma, o princípio da informação é um dos mais relevantes para o tratamento de dados, sendo verificado ao longo de toda a Lei, uma vez que essas atividades sempre dependerão de informações a serem previamente fornecidas ao consumidor usuário, devendo estar contidas nos contratos de prestação de serviço ou termos de aplicação de uso de modo destacado, claro e objetivo, que permita o esclarecimento ao contratante para que este dê seu devido consentimento qualificado, sem o qual o tratamento não terá validade. Complementarmente, a importância da informação no âmbito de validade dos contratos se deve muito ao contexto social, tecnológico e econômico atual, componentes da sociedade de consumo:

> Hoje o contrato é informação, daí a importância de sua interpretação sempre a favor do contratante mais fraco e das expectativas legítimas nele criadas por aquele tipo de contrato. Neste momento, o elaborador do contrato e aquele que o utiliza no mercado de consumo [...] devem ter em conta o seu dever próprio de informar, que inclui o dever de redação clara e com destaque, além do dever de considerar a condição

> leiga do outro, evitando dubiedades na redação contratual (MARQUES, 2006).

Não obstante, o princípio da informação possui desdobramentos atinentes à maioria dos preceitos expressos no art.6.º da LGPD. Ademais, como já ressaltado ao longo desta monografia, o princípio da informação dialoga reciprocamente com o princípio da confiança, além de ser um dos deveres anexos à boa-fé. Todos estes guardam relevância para as relações de consumo, estando contidos no CDC, e agora possuem aplicação fortalecida ao tratamento de dados pessoais, devido ao reforço da Lei n.º 13.709/2018.

Atente-se que no caput do art.6.º da LGPD optou-se por constar literalmente o princípio da boa-fé como regente das atividades de tratamento de dados. O uso da boa-fé como parâmetro das operações é uma escolha sábia, tendo em vista que, como já retratado ao longo deste trabalho, o princípio referido possui caráter amplo, envolvendo a realização de deveres anexos como lealdade, honestidade e informação, além de prezar pela prática de condutas idôneas e justas com as quais busca-se o atendimento das expectativas do contratante, *in casu* o titular dos dados tratados (KLEE, 2011).

No que tange a tutela de proteção de dados pessoais, a boa-fé como dever orientador, de forma abrangente, das relações entre titulares e agentes de tratamento possui ainda mais importância diante do cenário em que nos encontramos, no qual o tratamento de dados vêm ocorrendo em larga escala por meio de mecanismos já massificados e tendo em mente a falta de materialidade e dificuldade de controle inerente a estas atividades (DONEDA; MENDES, 2018).

Por sua vez, o princípio da finalidade obriga que o tratamento de dados obedeça a um fim, previamente firmado e conhecido pelo titular. A finalidade da operação de tratamento, servirá como justificativa de sua ocorrência e será vinculante para seu procedimento de legalidade, desta feita, os legisladores da LGPD optaram por firmar o entendimento de que os dados pessoais não podem ser tidos como mera "coisa comercial", logo, todo tratamento de dados deve possuir uma função e utilidade, não podendo ser efetuado indiscriminadamente e imotivadamente (OLIVEIRA, 2018). Por isso, o conhecimento da finalidade do tratamento pelo titular é elemento essencial para a validade da operação:

> [...] Ainda, qualquer alteração na finalidade da coleta deverá ser objeto de consulta e, se for o caso, novo consentimento do titular, pois o princípio da finalidade está relacionado com a privacidade informacional e, na hipótese de alteração, o titular pode não concordar com o novo caminho que seus dados percorrerão, o que violaria a autodeterminação informativa (SANTOS; TALIBA, 2018).

Outrossim, outros princípios expressos no art.6.º da LGPD não possuem necessariamente relação direta com o princípio da informação, mas não deixam de ser extremamente relevantes, uma vez que podem ser aplicados a situações específicas e recorrentes no tratamento de dados pessoais: as práticas abusivas. Nesse grupo, toma-se de exemplo o princípio da não discriminação e da responsabilização e prestação de contas, os quais simbolizam a preocupação da Lei Geral de Proteção de Dados com as novas demandas concernentes às práticas de mau uso e manipulação de dados pessoais que vêm atingindo os usuários da internet com maior frequência, podendo ser citada como exemplo a prática de: *profiling*, que utiliza dados pessoais captados de um indivíduo para bolar propagandas personalizadas, muitas vezes sem o conhecimento ou desejo do titular em recebê-las.

A Lei ao vedar a discriminação pelo tratamento de dados, reconhece a potencial utilização do conhecimento a respeito de dados de alguém para fins discriminatórios, excluindo ou categorizando o usuário com base em suas informações pessoais. Já o princípio da prevenção possui como objetivo maior de evitar os danos causados ao usuário pelo tratamento de dados, por meio da elaboração de medidas que promovem, acima tudo, o respeito à privacidade do titular (MULHOLLAND, 2018).

O art.6.º, X da Lei 13.709/2018, encerra o rol de princípios expressos do tratamento de dados com o princípio da responsabilização e prestação de contas. Implica concluir que, caso não ocorra o devido cumprimento de todas as obrigações devidas para a legalidade do tratamento de dados nem a adoção de medidas capazes de comprovar a observância às normas de proteção de dados, caberá certamente a responsabilização do agente de tratamento por seus atos. Este último princípio guarda extrema importância para a estabilidade das relações jurídica firmadas no meio virtual e para a construção de um regime jurídico de proteção de dados realmente capaz de proteger os sujeitos mais afetados, garantindo, ainda, o prosseguimento do tratamento de dados como atividade econômica lícita.

4 A RESPONSABILIDADE CIVIL NO COMÉRCIO ELETRÔNICO

Consoante o ensinamento de Guilherme Magalhães Martins (2014), o instituto da responsabilidade civil ficou por muito tempo ficou restrito ao Direito Civil e suas relações contratuais e, portanto, teve de passar por um processo de adaptação ao integrar-se a tutela das relações de consumo a fim de atender as suas necessidades. Isto porque, a partir da revolução industrial, a produção dos bens de consumo passou a ser feita em série, assim como criaram-se instrumentos para a facilitação da distribuição dos bens em massa. Nessa senda, o aumento da potencialidade danosa acarretou a transformação do referido instituto, o qual não poderia ater-se apenas à relação entre partes individuais e iguais, exigindo-se a partir daquele momento a "regulamentação da vida social", sendo necessária a proteção de direitos inerentes a toda uma coletividade. Com vistas à essa questão, a responsabilidade civil no Direito do Consumidor passou a adotar características mais protetivas da dignidade que tutela mais amplamente, diferenciando-se do regime de responsabilização padrão adotado como regra no âmbito civil.

Prezando pelo mesmo raciocínio, Gustavo Tepedino, ainda no prefácio da obra "Responsabilidade Civil por Acidente de Consumo na Internet", redigida por Martins (2014), acertadamente pontua que o fato de ser tão inusitado o potencial lesivo das tecnologias de informação pode originar uma extensa quantidade de eventos, multifacetados, complexos e constante em transformação, causando variados danos às pessoas e culminando sempre em especial o risco de violação de sua intimidade e privacidade de formas nunca vistas antes. Num cenário como esse, a antiga forma atribuída, historicamente, aos instrumentos jurídicos firmados, voltados a segurança patrimonial, são inadequadas em face das possibilidades únicas de atuação no meio virtual. Assim, tais circunstâncias exigem novas formas de autenticação formal, objetivando, além da proteção do patrimônio, a proteção de valores amplos e inerentes da pessoa humana, tais como a identidade pessoal, honra, informação, privacidade etc.

Nesta toada, Maria Celina Bodin de Moraes elucida que há um novo "propósito" da responsabilidade civil, no qual o eixo da obrigação que se desloca do "ofensor de responder por suas faltas para o direito da vítima de ter reparadas suas perdas, tal fator aliado ao imperativo da solidariedade social (...) impõe a intensificação de critérios objetivos de reparação" (MORAES *apud* MARTINS, 2014).

Outrossim, tendo em vista a contínua evolução da produção de bens e serviços e sua distribuição cada vez mais ampla, facilitada pela era digital em que nos situamos, a efetiva reparação de danos, apresenta-se na seara consumerista como direito fundamental, previsto no art.6.º, VI do CDC, abrigando o princípio da reparação integral. Este princípio prega a

reparabilidade ampla dos danos causados, sejam estes diretamente ou indiretamente decorrentes do fato (MIRAGEM, 2016). Tal previsão, entretanto, não exclui a necessidade de que se realize a análise da relevância jurídica do dano para que se verifique o dever de indenizar compatível, devendo ser demonstrado no caso concreto, principalmente quando se tratar de danos não patrimoniais, o mérito da proteção daquele interesse. Assim sendo, a efetiva reparação não significa que terá aplicação irrestrita, até porque isso resultaria numa oneração da sociedade como um todo, a qual deveria arcar com a distribuição dos riscos e do preço da segurança, de forma que os próprios consumidores sairiam prejudicados eventualmente (VINEY; JOURDAIN *apud* MARTINS, 2014).

Destarte, é certo que a responsabilidade civil é um instituto plenamente reconhecido no Direito do Consumidor, de modo que existem diversos artigos que fazem referência à possibilidades de responsabilidade do fornecedor, sendo adotada no direito brasileiro a regra geral de responsabilização solidária e objetiva dos fornecedores, tal como exemplificado pelos artigos 7.º, parágrafo único e artigo 12 do Código de Defesa do Consumidor (GMACH, 2018).

A utilização da responsabilidade objetiva e solidária acaba por trazer desdobramentos necessários e mais favoráveis ao consumidor no comércio eletrônico, tendo em vista a situação de vulnerabilidade agravada em que se encontra o indivíduo diante do modelo de contratação praticado no âmbito virtual, assim como, diante do meio utilizado, qual seja, a internet. Uma vez que este meio possui de características capazes de representar graves entraves à fiscalização e controle do cumprimento das obrigações contratuais, dentre as quais frisa-se a impessoalidade da relação entre as partes, torna-se comum a ocorrência de práticas abusivas contra o consumidor. Culminado à isso, muitas vezes, é impossível verificar a identidade, localização e idoneidade do fornecedor de bens e serviços na internet, estando o consumidor sujeito a receber informações falsas ou maliciosas do fornecedor, consequentemente a satisfação das demandas e reclamações do consumidor, em caso de prejuízos decorrentes deste tipo contratação, também costuma ser afetada negativamente (MARQUES, 2006).

> A ausência de uma regulação, tratando-se de relações de consumo cuja insegurança e risco avultam, num meio eletrônico reconhecidamente passível de violação por meio de uma rede aberta, como a Internet, agrava o quadro da vulnerabilidade do consumidor, tido como a mais fraca das partes envolvidas. Diante disso não pode ser recusada aplicação às normas da Lei 8.078/90, erigidas ao status de garantia constitucional e princípio geral da ordem econômica, respectivamente, na forma dos arts.5, XXXII e 170, V, da CF/1988 (MARTINS, 2014).

Após todo exposto nesta monografia, sabe-se que o Código do Consumidor vem sido

plenamente aplicável às relações de consumo no *e-commerce*. A conhecida B2C (*Business to Consumer*) é parte do grupo composto por três relações jurídicas consideradas as mais importantes no meio virtual em conjunto com a B2B (*Business to Business*) e B2G (*Business to Government*). Como o próprio nome sugere, a B2C diz respeito às relações jurídicas ocorridas entre consumidor e fornecedor, enquanto as demais versam sobre as relações comerciais entre duas pessoas físicas ou duas pessoas jurídicas sem elemento consumerista (B2B) e relações de consumo envolvendo pessoas jurídicas de direito público ou de direito privado prestadoras de serviço público ou instituídas por lei (B2G). No que tange a responsabilidade civil, haverá diferenciação entre as modalidades, devendo ser aplicado o modelo de responsabilidade subjetiva às relações B2B conforme o art.927, parágrafo único do Código Civil, analisando a culpa, dano e nexo causal para sua configuração. Já nas modalidades B2C e B2G será aplicada a responsabilidade objetiva, uma vez configurada vulnerabilidade da parte consumidora na relação, independendo da análise da culpa para sua constituição, consoante previsão do Código de Defesa do Consumidor e do art.37, §6.º da Constituição Federal para as citadas modalidades respectivamente (CASTRO; VIEGAS, 2016).

Isto posto, a responsabilidade objetiva dos fornecedores nas relações B2C no *e-commerce* baseia-se na concepção consolidada no CDC cuja fundamentação dá-se pela aplicação da Teoria do Risco Empresarial, ou Teoria do Risco da Atividade, na qual cabe ao fornecedor arcar com as maiores responsabilidades da relação. Por isso, observa no Código de Defesa do Consumidor o estabelecimento de uma série de padrões de qualidade, prazos e sansões a serem observados pela parte fornecedora, aplicáveis igualmente ao comércio físico e ao *e-commerce* (CASTRO; VIEGAS, 2016).

Apesar disso, hodiernamente, muito embora a existência de diversos dispositivos no Código do Consumidor que estabelecem a justa responsabilização dos fornecedores e a ampla e efetiva reparação dos danos, surgem todos os dias na internet novas situações que exigem amparo diferenciado, de modo que os consumidores continuam a ter seus direitos violados com frequência superior no comércio eletrônico. Destarte, é inegável a importância da construção de leis específicas que tenham como objeto as relações jurídicas virtuais, tais como a LGPD e o Marco Civil da Internet, entre outras, uma vez que estas servem de auxílio no fortalecimento do instituto de responsabilização naquela seara, no sentido de que, em tese, seriam melhores em abrangir as peculiaridades daquele meio ao estabelecer princípios e novas obrigações para as partes/agentes, por conseguinte, desenvolvendo novas possibilidades de responsabilização necessárias para a eficácia da responsabilidade civil e reparação de danos no contexto cibernético.

4.1 A responsabilidade civil na Lei geral de Proteção de Dados

Para melhor compreensão da responsabilidade civil na Lei Geral de Proteção de Dados, retomaremos a previsão do art. 6.º, inciso X, da referida Lei, o qual versa que, dentre os princípios norteadores das atividades de tratamento de dados, se encontra a "responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas" (BRASIL, 2018).

Desta forma, a partir da adoção da responsabilização como princípio, entende-se que todas as relações e operações relacionadas ao tratamento de dados deverão se pautar, inevitavelmente, no atendimento deste dever de agir. Posteriormente, a LGPD dedica sessões específicas à questão da responsabilidade, quais sejam a Sessão II do Capítulo IV, que abrange os artigos 31 e 32, a Sessão III do Capítulo VI, que inclui os artigos 42 a 45. Igualmente, cabe ser citada a Sessão I do Capítulo VIII, o qual dispões as sanções administrativas aplicáveis a partir da ocorrência de violação às normas daquele instrumento legal.

O supracitado Capítulo IV, diz respeito ao tratamento de dados pessoais efetuado pelo Poder Público, de modo que os artigos 31 e 32 são os únicos dispositivos a fazer referência direta à possibilidade de responsabilização destes agentes de tratamento, neste caso, agentes públicos. Aqui cabe apenas citar a linguagem genérica adotada pela lei, que se limitou a declarar: "Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação" (BRASIL, 2018) , sendo esta a redação do art.31. O art.32, seguindo a mesma linha, atribuiu à Autoridade Nacional de Proteção de Dados, entidade criada pela própria LGPD, a solicitação de publicação de relatórios relacionados ao impacto na proteção de dados pessoais e o dever de sugerir a adoção de padrões e de boas práticas no tratamento de dados efetuados por agentes do Poder Público.

Não obstante, o entendimento a ser firmado nesse trabalho considera preocupante a generalidade dos dispositivos supracitados, por não considerar que foi levada em apreço a real extensão de riscos propiciados ao cidadão no tratamento de dados pessoais efetuados pelo Poder Público, basta refletir sobre o grande abismo técnico, econômico e de poder entre as partes em questão. Assim como são amplas as hipóteses firmadas pela Lei, em que é legitimo o tratamento de dados realizado pelo Estado, dessa forma considera-se mais razoável que a Lei, firmasse desde logo ,de maneira expressa, um dever específico ao Poder Público , a partir da configuração da responsabilidade objetiva por violações aos princípios e regras do tratamento

de dados, ao invés de apenas atribuir à autoridade nacional a possibilidade, e não dever, de enviar informe com as medidas cabíveis para cessar a violação.

Ademais, junta-se como agravante dessa circunstância o fato de que a medida provisória (MP 869/2018) acabou justamente revogando a possibilidade de que a Autoridade Nacional de Proteção de Dados (ANPD) pudesse "emitir opiniões técnicas ou recomendações e solicitar relatórios de impacto à proteção de dados pessoais aos órgãos de segurança" (SENADO NOTÍCIAS, 2019), perdendo força o art.32 da Lei Geral de Proteção de Dados, num contexto em que apenas dois artigos da Lei versam diretamente sobre a responsabilidade do Estado no tratamento de dados pessoais.

Quando analisada de maneira comparativa, a responsabilidade civil aplicada à particulares e à agentes públicos, percebe-se que o legislador optou, em relação aos primeiros, por previsões específicas e mais detalhadas, objetivando atingir principalmente as pessoas jurídicas atuantes no meio virtual, as quais são, em sua maioria, partes nas relações de consumo como fornecedoras de bens e serviços. Portanto, diante das possibilidades e responsabilidades dispensadas ao Poder Público, os particulares encontram-se numa situação que exige mudanças mais complexas em sua maneira de atuação, sendo necessária sua adequação às novas disposições, assim como a conjugação com previsões legais já consagradas como o Marco Civil e o Código de Direito do Consumidor.

As diferenças relatadas acima, podem ser constatadas de início, no caput do art.42 da Lei, que ao comparar-se com o já mencionado art.32, é possível notar clara diferença de tratamento. No primeiro dispositivo supracitado, foi estabelecido, além dos tipos de danos possíveis no tratamento de dados pessoais, também o modelo de responsabilidade atribuída aos agentes específicos de tratamento, quais sejam os operadores e controladores (art.42, §1º, incisos I e II, LGPD). Ademais é importante frisar, a possibilidade de inversão do ônus da prova em favor do titular de dados (art.42, §2º), reforçando a ideia de que o indivíduo costuma ser a parte mais vulnerável e hipossuficiente em face de grandes empresas do âmbito virtual. Enfim, merece igual reconhecimento positivo, a disposição expressa no parágrafo §3º do art.42, sobre a possibilidade de responsabilização por danos coletivos.

O art. 43, contido na mesma Sessão III do Capítulo VI, intitulado "Dos agentes de tratamento de dados pessoais", prevê ainda as hipóteses de não responsabilização dos agentes, quais sejam, mediante comprovação: de que não realizaram o tratamento de dados pessoais que lhes foi atribuído; de que embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados ou de que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros (BRASIL, 2018). É evidente a relação

dessas hipóteses com aquelas dispostas no CDC, nos incisos de seu art.12, § 3º.

Considera-se proveitosa, portanto, a consonância entre a Lei Geral de Proteção de Dados e o Código de Direito do Consumidor, tendo a Lei, inclusive reforçado literalmente a aplicação das normas consumeristas no caso de o tratamento de dados envolver relação de consumo, logo, de acordo, com o art. 45. "As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente" (BRASIL, 2018).

Pelo exposto, a LGPD realmente foi inovadora ao tratar expressamente e particularmente sobre a responsabilidade civil no tratamento de dados pessoais, dando o enfoque necessário à responsabilização de agentes específicos, de forma a conjugar os princípios e demais normas do ordenamento jurídico brasileiro e legislações internacionais, a favor responsabilidade objetiva, considerando os direitos fundamentais interligados às operações de tratamento e a potencialidade danosa gigantesca oriunda do ambiente cibernético.

Por outro lado, deixou de preocupar-se efetivamente com o tratamento de dados efetuado pelo Poder Público, pois, embora o tratamento de dados seja essencial à atividade pública, na sociedade atual não é incomum que o poder de controle e monitoramento característico do Estado se sobreponham à privacidade e intimidade do indivíduo de formas nem sempre legitimas. Como exemplo extremo da capacidade de controle e utilização das informações pessoais dos cidadãos pelo Estado, têm-se o caso da China, que em 2014, anunciou um "sistema de crédito social", com implementação até 2020, a ser gerido e mantido pelo governo chinês. Por meio desse sistema, "será possível categorizar e taxar os comportamentos dos cidadãos como positivos ou negativos (na visão do Estado), indicando uma classificação única e pública daquela pessoa, que servirá para determinar se um cidadão terá direito ao acesso a determinadas políticas públicas" (MULHOLLAND, 2018).

> Dessa feita, há também de se vislumbrar que o alcance dos dados em geral se multiplicou em escalas outrora jamais imaginadas, porém, não há só benefícios nesse processo, uma vez que há uma clara tendência de diminuição da esfera privada dos cidadãos, comumente observada, por exemplo, no crescente hábito de sempre estarmos sendo filmados, seja pela autoridade pública, seja por particulares, sedentos por partilhar seu cotidiano com os seus amigos virtuais em redes sociais das mais variadas (RODRIGUES; FERREIRA, 2019).

Por conta de situações como esta, a possibilidade de responsabilidade civil atribuída aos agentes públicos deve ser firmada em bases legais que compatibilizem acertadamente os deveres e necessidades do Estado em relação aos dados pessoais de seus jurisdicionados com

os direitos atribuídos a estes, na condição titulares de seus dados, pelo resto do ordenamento jurídico.

4.1.1 As obrigações dos agentes de tratamento

Inicialmente, é cabível destacar que a Lei Geral de Proteção de Dados define o tratamento de dados de forma ampla, abrangendo diversas operações informáticas, conforme o art.5.º, inciso X, da Lei. Por outro lado, os agentes de tratamento são definidos de maneira restrita no art.5.º, inciso IX, no qual apenas controladores e operadores foram considerados. Ademais a LGPD menciona, no mesmo artigo (inciso VIII) a figura do encarregado, o qual, apesar de não ser considerado agente de tratamento, será uma pessoa natural escolhida pelo controlador para agir como canal de comunicação entre os titulares de dados, o próprio controlador e a autoridade nacional de proteção de dados.

A partir da leitura do art. 5.º da LGPD, abstém- se a noção de que, no que tange os agentes de tratamento de dados, o controlador é a figura mais poderosa:

> Art. 5º Para os fins desta Lei, considera-se:
> [...]
> VI - **controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais**;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que **realiza o tratamento de dados pessoais em nome do controlador**;
> [...]
> (BRASIL, 2018, grifos nossos).

Portanto, o controlador seria aquele com a maior gerência sobre os dados a serem tratados, definindo a operação a ser utilizada e seus fins, enquanto o operador é aquele que dará andamento ao tratamento a partir das decisões do controlador. A citada definição é vaga e de difícil idealização para quem não é versado nos aspectos técnicos da tecnologia de informação, tornando difícil para o indivíduo comum situar quem são os agentes de tratamento da relação virtual em que é parte, mais difícil ainda seria discernir quem é o controlador e quem é o operador num contexto prático.

Neste ensejo, exemplarmente, podemos relacionar os provedores de internet com a figura do controlador, como forma de melhor ilustrar sua posição no tratamento de dados pessoais, visto que os provedores utilizam-se de informações de seus usuário, seja com fins econômicos ou não, para realizar variadas operações e fornecer uma série de funcionalidades e serviços, os quais podem ser acessados a partir de máquina conectada a rede mundial de

computadores (AQUINO *apud* SANTOS; DUARTE, 2018). Assim os provedores de aplicação de internet (PAI), como são conhecidos, mas que também atendem pela nomenclatura "provedores de conteúdo", podem ser conceituados da seguinte forma:

> O provedor de conteúdo, finalmente, é toda pessoa natural ou jurídica que disponibiliza na Internet as informações criadas ou desenvolvidas pelos provedores de informação, utilizando servidores próprios ou os serviços de um provedor de hospedagem para armazená-las (LEONARDI *apud* SANTOS; DUARTE, 2018).

Fica claro, partindo da conceituação acima que os provedores de aplicação de internet, poderiam se encaixar facilmente na função de controladores no tratamento de dados, tendo em vista que se utilizam da conexão do usuário com a internet para oferecer as funcionalidades disponibilizadas por meio de serviços de acesso gratuito ou oneroso aos usuários. Desta maneira, os provedores de aplicação de internet possuem como característica intrínseca coleta, armazenamento e processamento de dados, ou seja, o tratamento de dados, como forma de fomento aos seus serviços e funções (SANTOS; DUARTE, 2018).

Na seara consumerista, é requisito a remuneração pelo serviço, havendo ganhos financeiros ao fornecedor no mercado de consumo. A remuneração do fornecedor pode se dar tanto diretamente, a partir do pagamento do próprio consumidor, quanto indiretamente, quando a remuneração vem de outros empresários, tal como nos casos de publicidade, ou nos casos de acesso à internet gratuita (MARQUES, 2004).

O que se constata ao se tratar de serviços ofertados gratuitamente na internet é que esta "gratuidade" é meramente ilusória, pois além de verificada a possibilidade de remuneração indireta destes fornecedores por meio da publicidade, não se pode esquecer o valor atribuído às informações dos usuários armazenadas por estes no contexto atual (MARTINS, 2014). Estes dados que, majoritariamente, são coletados sem custo, e até sem o conhecimento dos titulares, como efeito colateral de sua relação com o fornecedor, possuem valor econômico extremamente relevante na sociedade moderna, podendo gerar lucro a estes fornecedores pela troca, venda, publicidade individualizada entre outras práticas que se tornam muitas vezes abusivas.

> (...) É justamente o movimento da análise econômica nos Estados Unidos que nos alerta para a falácia 'econômica' dos chamados 'serviços', 'utilidades' ou promessas 'gratuitas', o que não passaria de uma superada ficção jurídica. O que parece juridicamente gratuito (...), é economicamente baseado na certeza de remuneração indireta, na interdependência de prestares futuros e atuais (sinalagma escondido), no estado de catividade e de dependência a que um dos parceiros fica

> reduzido e no lucro direto e indireto do outro (...) (MARQUES, 2004).

Sob essas premissas, têm-se que os agentes de tratamento, em especial os controladores, serão, no caso de uma relação virtual de consumo, a parte fornecedora que decidirá quais as operações a serem realizadas com os dados do contratante e de que forma serão utilizados posteriormente para a obtenção de retorno financeiro. Igualmente, é necessário que os agentes de tratamento cumpram as obrigações atribuídas a si pela Lei Geral de Proteção de Dados e sejam responsabilizados civilmente caso violem os princípios e regras do tratamento de dados.

Ante o exposto, a Lei Geral de Proteção de Dados estabeleceu os limites ao tratamento de dados e procedimentos especiais para sua realização, com o fulcro de propiciar segurança e reforçar as garantias dos titulares de dados. Isto pode ser constatado por meio da atribuição de obrigações aos agentes de tratamento, designando instrumentos para defesa, proteção e prevenção de danos ao titular no tratamento de dados. Além disso, nota-se que o controlador é o sujeito que detém mais poder e, por conseguinte, mais reponsabilidades; já no art.41 da LGPD é dispensado ao controlador o dever de instituir um encarregado pelo tratamento de dados, o qual deverá atuar como agente comunicador de reclamações dos titulares, realizador de orientações aos funcionários e responsável por estabelecer uma ponte entre as partes e a Autoridade Nacional (DONEDA; MENDES, 2018).

Segundo entendimento de Doneda e Mendes (2018), o Capítulo VII que trata da segurança da informação, e contém os artigos 46 ao 51 da LGPD, traz inovações essenciais ao ordenamento jurídico brasileiro quanto às obrigações dos agentes de tratamento. O art.46 da Lei Geral de Proteção de Dados, firma como obrigação dos agentes de tratamento a adoção de medidas: de segurança; técnicas e administrativas, capazes de proteger os dados pessoais contra acessos não autorizados de terceiros, situações acidentais ou atos ilícitos que possam causar perda, destruição, alteração, divulgação ou qualquer forma inadequada de tratamento de dados. Concomitantemente, o art.48 da Lei encarrega novamente o controlador de função essencial, ao definir que este será responsável pela comunicação ao titular e à Autoridade Nacional, em caso de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (BRASIL, 2018).

Inclui-se dentre as obrigações do controlador aquela extraída do art. 38, na qual deverá realizar um relatório de impacto à proteção de dados pessoais, referente as operações de tratamento de dados realizadas sobre sua gerência. O relatório, solicitado pela ANPD, deverá conter uma descrição da operação de tratamento de dados pessoais, as medidas que tenha

adotado na coleta e segurança dos dados e a análise do controlador em relação aso risco presente do tratamento realizado.

A Lei Geral de Proteção de Dados reafirma a subserviência do agente operador em relação ao controlador diversas vezes. O art. 39 prevê que o operador "deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria" (BRASIL, 2018). Infere-se, portanto, outra obrigação do controlador, qual seja a análise de conformidade de suas instruções para com as normas do ordenamento jurídico brasileiro, percebe-se, de fato, que a LGPD atribuiu ao controlador a responsabilidade quase total pelos riscos da atividade.

Nesse sentido, segundo o art.42, §1º, inciso I da supracitada lei, "o operador somente será responsabilizado por atos que cometa e que sejam contrários à Lei ou às instruções que lhe sejam fornecidas pelo controlador, casos nos quais aplica-se o regime de responsabilidade solidária entre controlador e operador" (DONEDA; MENDES, 2018). Já o controlador, ficará responsável pelas demais hipóteses.

A reponsabilidade solidária também é aplicada nos casos envolvendo mais de um controlador (art. 42, § 1º, II), seguindo o objetivo de reparar efetivamente o titular dos dados. Apesar da existência dessas hipóteses, a LGPD não dispõe o regime de responsabilização solidária como regra, todavia, firma especificamente a necessidade de observância das regras de responsabilidade previstas em legislação pertinente, caso se configure relação consumerista (art.45). Isto é, aplicar-se-á o regime de responsabilidade objetiva e solidária contida no CDC, como regra, quando a violação ao direito do titular se der no âmbito de uma relação de consumo.

4.1.2 A criação da Autoridade Nacional e as repercussões da LGPD na atividade empresarial

Indiscutivelmente, a maior inovação da Lei Geral de Proteção de Dados foi a criação de um órgão da administração pública federal exclusivamente dedicado à proteção de dados pessoais: a Autoridade Nacional de Proteção de Dados (ANPD), contida no Capítulo IX da Lei. Entretanto, à época em que foi sancionada, a LGPD teve vários artigos vetados, incluindo os artigos 55 a 59, os quais versavam especificamente sobre a criação da ANPD e demais aspectos referentes à sua atuação e composição, sob fundamento de que os referidos dispositivos incorreram em vício de iniciativa, tal como dispõe o art. 61, § 1º, II, em conjunto com o art. 37 da Constituição Federal.

O veto logo se mostrou extremamente problemático, tendo em vista que o referido órgão "não é um mero coadjuvante do sistema de proteção de dados: ao contrário, é o seu pilar de sustentação, sem o qual todo o arcabouço normativo e principiológico não está apto a

funcionar de forma adequada" (DONEDA; MENDES, 2018). Com efeito, são inúmeras as situações previstas pela LGPD em que a Autoridade Nacional deve atuar, sua participação dá-se desde os primórdios da atividade de tratamento, por meio da solicitação e análise de relatórios de impacto à proteção de dados, perpassando pela competência de determinar medidas de segurança; sanções administrativas; medidas de reversão de efeitos nos casos de vazamento de dados, entre outras funções. A ANPD também poderá regular padrões técnicos de segurança da informação e autorizar transferências internacionais, sendo estas apenas algumas das diversas competências que lhe são atribuídas. Ante o exposto, a Autoridade Nacional de Proteção de Dados tem seu lugar como elemento chave para garantia da proteção efetiva dos titulares dos dados e do tratamento de dados como atividade econômica.

De fato, a criação de um órgão dedicado exclusivamente à matéria permite ao Brasil a materialização de um regime jurídico de proteção de dados com grande potencial efetivo. Não é por outra razão que grande parte dos países do mundo possuem autoridades similares, a Alemanha, Suécia e França, por exemplo, criaram seus respectivos órgãos ainda nos primórdios das discussões sobre proteção de dados nos anos 1970, enquanto na maioria dos países restantes a criação do órgão desenvolveu-se a partir das décadas de 1990 e 2000, o que, em regra, se deu em conjunto com a promulgação de leis específicas em âmbito interno (DONEDA; MENDES, 2018).

> (...)conforme o último censo da Conferência Internacional de Autoridades de Proteção de Dados e Privacidade (ICDPPC)12. Dados recentes indicam que, dos 120 países que possuem Leis de proteção de dados, apenas 12 não criaram uma autoridade independente responsável por sua aplicação e, por conta disto, são conhecidos internacionalmente como parte de um pequeno "corredor da vergonha" (GREENLEAF *apud* DONEDA; MENDES, 2018).

Neste ensejo, constatou-se grandes entraves à efetividade e aplicação da LGPD caso fosse impossibilitada a criação da Autoridade Nacional de Proteção de Dados, fato que geraria risco de que as ações e decisões dos agentes legitimados para atuar na proteção de dados se tornassem dispersas e conflitantes, tendo em vista a variedade de legitimados para atuar nesta seara no contexto em que se encontrava o país antes da criação da ANPD (DONEDA; MENDES, 2018). Desta feita, foi concebida a Medida Provisória n.º 869 de 2018 com intuito de retomar a fundação da Autoridade Nacional, agora como órgão da administração pública federal integrante da Presidência da República (art.55-A da LGPD), o que foi feito sem o

aumento de despesas, utilizando-se de cargos e funções de órgãos e entidades do Poder Executivo.

A Medida Provisória em questão alterou ainda alguns outros dispositivos não relativos diretamente à Autoridade Nacional, contudo, a grande maioria dessas modificações afetou apenas a utilização de termos e nomenclaturas específicas. Com relação à Autoridade Nacional de Proteção de Dados, grande parte de suas competências originais foi mantida, cabendo a esta: a edição de normas; zelar pela proteção; requisitar informações; registrar reclamações; fiscalizar; comunicar às autoridades e órgãos de controle interno sobre a existência de infrações penais e descumprimentos; formular estudos e padrões técnicos; elaborar relatórios; realizar a cooperação internacional, etc. Nessa senda, a MP n.º 869 estabeleceu a competência sancionatória exclusiva da ANPD e firmou a cooperação institucional, na qual a atuação da Autoridade Nacional deverá se pautar no diálogo com o Sistema Nacional de Defesa do Consumidor, o Ministério da Justiça e demais órgãos (BRASIL, 2018).

Ante o exposto, evidencia-se que Autoridade Nacional de Proteção de Dados guarda importante papel para o atingimento dos princípios estabelecidos pela Lei para o tratamento de dados. Nestes termos, o princípio da responsabilização e prestação de contas pode ser concretizado com base na atuação direta da ANPD, em especial, em se tratando da aplicação de sanções administrativas, conforme delimitam arts.52 a 54 da LGPD.

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III - multa diária, observado o limite total a que se refere o inciso II;
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI - eliminação dos dados pessoais a que se refere a infração;
> (BRASIL, 2018).

Notadamente, as hipóteses de responsabilidade civil concebidas pela Lei não possuem nada de muito inovador no sentido jurídico, correspondendo ao que se espera do arcabouço do Direito Privado brasileiro. Não obstante, é válido ressaltar que a previsão originária da LGPD acrescentava ao artigo supracitado os incisos VII; VIII e IX que traziam as hipóteses de:

suspensão (total ou parcial) do funcionamento de banco de dados; suspenção do exercício da atividade de tratamento dos dados e proibição (parcial ou total) do exercício de atividades relacionadas a tratamento de dados (BRASIL, 2018).

Destarte, a Medida Provisória veio para balancear e apaziguar certas críticas de setores da sociedade, tanto por meio da criação efetiva da Autoridade Nacional de Proteção de Dados quanto por meio do veto de certos dispositivos que poderiam causar maiores prejuízos a poderosos agentes econômicos, os quais dependem do tratamento de dados para fomento de suas atividades. A retirada dos mencionados incisos VII; VIII e IX do art.52 é apenas um dos exemplos, tendo em vista que estes dispositivos impediriam parcial ou totalmente a continuidade das atividades dessas empresas até que estas se regularizassem aos conformes legais. Neste cenário, a Lei Geral de Proteção de Dados continua a sofrer críticas por parte de alguns agentes econômicos, os quais consideram que certos dispositivos da Lei poderiam "empacar" a atividade empresarial no *e-commerce* , causando impactos negativos na atividade econômica de tratamento de dados, que já é uma das mais importantes no mercado virtual brasileiro. As principais críticas dizem respeito à questão da responsabilidade civil, pois considera-se que os valores estipulados para as multas, com ênfase no inciso II do art.52 da LGPD, que define o valor limite de cinquenta milhões de reais **por infração**, seriam extremamente impraticáveis e prejudiciais para a continuidade das atividades de micro e pequenas empresas, as quais representam boa parcela das pessoas jurídicas atuantes no comércio eletrônico (CONJUR, 2019).

Outrossim, a Lei Geral de Proteção de Dados precisará superar desafios para que seja aplicada com efetividade, a começar pela verdadeira mudança de cultura empresarial na lida com as atividades de tratamento de dados pessoais, pois a facilidade e a liberdade com que ocorrem, na atual conjuntura, certamente não serão mais as mesmas. A Lei 13.709/2018 passará a viger no dia 16 de fevereiro de 2020 e enquanto não chega esta data, as empresas deverão se adequar às exigências legais mais recentes e complexas trazidas pela LGPD, as quais demandarão bastante esforço e adaptação, tudo isto num espaço temporal relativamente curto (FRAZÃO, 2018).

A aludida mudança cultural muito diz respeito aos princípios da necessidade e da finalidade previstos na LGPD. Isto se deve ao fato de que o tratamento de dados fica restringido à hipóteses em que estas operações sejam realmente essenciais, ou seja, apenas para atender às necessidades do controlador de dados, além disso, a utilização, contexto e a forma do tratamento devem ser compatíveis com as finalidades para as quais os dados foram coletados. Deste modo, a mudança cultural exigida, perpassa pela necessidade de compreensão, por parte das empresas

e agentes de tratamento, de que os dados pessoais são totalmente merecedores da tutela jurídica específica, uma vez que se trata de "elemento constituinte da identidade da pessoa", compondo parte fundamental da personalidade do indivíduo que terá desenvolvimento privilegiado a partir do reconhecimento da dignidade humana (MULHOLLAND, 2018). Portanto, é imperativo que proteção de dados integre o arcabouço jurídico nacional, devido sua conexão com direitos humanos essenciais como o Direito à Privacidade e as liberdades individuais, mas também porque se constitui como peça chave para o sistema de proteção do consumidor em suas relações jurídicas virtuais. Tudo isto contribui para que a proteção de dados possa "ser vista como a soma de um conjunto de direitos que configuram a cidadania do novo milênio" (RODOTÁ *apud* MULHOLLAND, 2018).

A partir desses fundamentos, é indispensável que as empresas passem a buscar novos sistemas operacionais e a realizar investimentos nas áreas de *marketing*, tecnologia da informação (TI), jurídica, recursos humanos e logística, para que proteção de dados pessoais se desenvolva como parte integrante da política de *compliance* e integre a realidade diária do empreendimento . Os investimentos nessa seara, a partir da promulgação da LGPD, passam a se relacionar com a confiabilidade e credibilidade na empresa no mercado e aos olhos do consumidor usuário, bem como cumprem com o fim de evitar situações de risco e danos, tendo em vista que uma empresa que verdadeiramente garanta a segurança das informações pessoais daqueles que contratam seus serviços e que possua mecanismos eficientes para tal, ampara-se de maneira mais efetiva contra possíveis sanções administrativas e condenações por responsabilidade civil (SANTOS; TALIBA, 2018).

> A proteção de dados, a certificação e a criação de ambientes e tecnologias seguras é questão de qualidade mínima daquele fornecedor que quer oferecer seus serviços e produtos na rede global.
> [...]
> Aqui se trata de um problema de organização do modelo negocial dos fornecedores para atrair e ganhar a confiança dos consumidores (MARQUES, 2011).

Em última análise, comprovou-se que a Lei Geral de Proteção de Dados, fortalecida pela Autoridade Nacional de Proteção de Dados, representa uma evolução para a segurança no ciberespaço e para a proteção dos dados pessoais de seus usuários, os quais por muito tempo careceram de aporte específico. Todavia, deve ser reiterado que efetiva aplicação da LGPD dependerá da interpretação desta lei dentro de um sistema, do qual fazem parte os demais diplomas normativos que dispõem sobre tratamento de dados pessoais, aplicando, desta feita, o "diálogo das fontes", tal como concebido por Erik Jayme e difundido em solo nacional por

Cláudia Lima Marques, “possibilitando a aplicação simultânea dos princípios e regras gerais da LGPD com as regras setoriais” , tais como: o Marco Civil, a Lei de Cadastro Positivo, o Código do Consumidor, entre outras (DONEDA; MENDES, 2018).

Deste modo, a regularização da atividade de tratamento de dados, por meio da promulgação da Lei Geral de Proteção de Dados, em conjunto com a aplicação prática de outros instrumentos legais, permitirá a criação de um ambiente mais seguro a todos os indivíduos, proporcionando práticas menos danosas e mais responsáveis. Sendo assim, as boas práticas no tratamento de dados favorecem o atendimento às expectativas depositadas pelo cidadão, reforçando sua confiança, além de garantir aos próprios agentes de tratamento a segurança jurídica e a transparência necessárias para a continuidade de suas atividades econômicas (MARQUES, 2006).

Finalmente, firma-se o entendimento, na presente monografia, de que, uma vez cumpridas com afinco as obrigações e os princípios firmados pelo novo regime geral de proteção de dados brasileiro será possível atingir um novo nível de confiabilidade da sociedade nas tecnologias de informação e telecomunicações. Este novo patamar deve ser definido pela qualidade desta confiança, empoderando-se os consumidores e ampliando a proteção de seus direitos, na mesma medida em que se propicia maior competividade e inovação aos prestadores de serviços disponibilizados na internet, os quais devem estar comprometidos com a utilização legítima e transparente dos dados pessoais.

5 CONCLUSÃO

Ao longo deste trabalho foi apresentada a importância social, política e econômica atribuída aos dados pessoais na atualidade, fato que levou o tratamento de dados na internet a ser concebido como uma das atividades econômicas mais lucrativas e em maior expansão. Portanto, gerou-se a necessidade de que os ordenamentos jurídicos se adequassem a esta realidade com o fulcro de amparar corretamente os direitos fundamentais dos usuários de serviços disponibilizados na internet. Desta feita, sabe-se que a inserção do Brasil neste contexto, se deu paulatinamente, culminando na promulgação da Lei Geral de Proteção de Dados (LGPD), de forma a inaugurar um sistema nacional de proteção de dados. A partir daí, constatou-se que a melhor forma de interpretação do referido sistema, deve ter como base a noção do " diálogo das fontes", tal como concebido por Erik Jayme e fomentado por Cláudia Lima Marques, para que os mais diversos instrumentos normativos e princípios que tratam sobre a mesma seara possam ser aplicados concomitantemente, em complementariedade, visando atingir a melhor garantia de direitos e proteção possíveis aos titulares de dados.

Igualmente, para que o ambiente virtual seja pautado por melhores práticas, deve ser levado em consideração, além das disposições legais, o atendimento às justas expectativas dos consumidores em relação ao cumprimento das obrigações contratuais e às condutas idôneas por parte do fornecedor. Logo, os princípios da boa-fé e seus deveres anexos, como o dever de informar e o dever de cooperação, detém grande relevância para a melhor elaboração de contratos de *e-commerce*, garantindo que o consumidor dê seu consentimento qualificado, ao invés de aderir "cegamente" as cláusulas contratuais.

Confirmou-se, ainda, o entendimento de que não se pode deixar que práticas abusivas de tratamento de dados continuem a afetar a segurança e privacidade dos consumidores nos contratos de *e-commerce*. Desta feita, veio em bom momento o sancionamento de uma lei específica brasileira, que versa mais afundo sobre as práticas abusivas decorrentes dessas operações e que apresenta uma melhor definição dos agentes que as perpetuam.

Neste cenário, a responsabilidade civil é um instituto essencial no comércio eletrônico, de modo a permitir que seja reparado efetivamente os danos causados aos consumidores usuários. Sobre esse aspecto, conclui-se que a Lei Geral de Proteção de Dados representa a necessária inovação do ordenamento jurídico brasileiro, trazendo previsões específicas de responsabilidade conforme os agentes de tratamento e suas respectivas funções, tendo adotado acertadamente o modelo de responsabilidade civil objetiva.

Seguindo essa linha, a LGPD criou a Autoridade Nacional de Proteção de Dados para materializar a aplicação de sanções administrativas, entretanto, a Lei ainda carece de disposições passíveis de resguardar mais eficientemente o indivíduo frente ao poderio técnico, econômico e informacional do Estado na lida com os dados pessoais de seus cidadãos.

Deste modo, construiu-se nesta monografia o posicionamento de que a efetividade da proteção de dados no Brasil, depende, primordialmente, da conciliação entre diversos fatores. A adequada aplicação do arcabouço jurídico desenvolvido sobre está problemática, no qual se inclui a própria Lei Geral de Proteção de Dados em diálogo com o Código do Consumidor, o Marco Civil da Internet, a Lei de Acesso à Informação etc., é um deles. Assim como, o adequado funcionamento da Autoridade Nacional de Proteção de Dados também é essencial, da feita que este órgão será o principal responsável pela fiscalização das atividades de tratamento de dados, de seus agentes e aplicará as medidas de responsabilização cabíveis com o fulcro de reparar os danos causados aos titulares.

Finalmente, não se pode olvidar que não bastará a previsão específica de responsabilidade civil se os principais atores da atividade de tratamento de dados não se adequarem ao novo sistema. Isto posto, o último fator é representado pela transformação na cultura empresarial, de forma que as empresas devem estimular a adoção de medidas preventivas, situando a questão da proteção de dados em suas políticas internas e *compliance* e ampliando a noção de segurança informacional contra possíveis ataques externos e negligências internas. Nestes termos, a Pessoa Jurídica que busque verdadeiramente se adequar às previsões legais e que, internamente, paute-se em boas condutas e práticas idôneas, garantindo a segurança às informações pessoais daqueles que contratam seus serviços e atendendo à essencial confiança dos consumidores, amparar-se-á de maneira mais efetiva contra a responsabilização por danos, que por ventura venham a ser causados, além de permitir o fortalecimento do tratamento de dados como atividade econômica.

REFERÊNCIAS

BBC. **O escândalo de uso político de dados que derrubou o valor do Facebook e o colocou na mira de autoridades.** São Paulo. 2018. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml. Acesso em: 31 out. 2018.

BBC. **Roubo de dados da Ashley Madison expõe cidade como capital da infidelidade. São Paulo**. 2016. Disponível em: http://g1.globo.com/tecnologia/noticia/2015/07/roubo-de-dados-da-ashley-madison-expoe-cidade-como-capital-da-infidelidade.html. Acesso em: 31 out. 2018.

BORGES, Gabriella Müller**. Contratos no Comércio Eletrônico e a Proteção do Consumidor no Século XXI:** Responsabilidade Civil dos Sites Intermediadores no *E-Commerce.* 2018. Trabalho de conclusão de Curso (Bacharel em Ciências Jurídicas e Sociais) - Universidade Federal do Rio Grande do Sul, Porto Alegre, 2018.

BRASIL**. Lei n.º 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei n.º 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 14 abr. 2019.

BRASIL. **Lei n.º 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L8078.htm. Acesso em: 3 maio 2019.

CASTRO, Maria Fernanda de Melo; VIEGAS, Cláudia Mara de Almeida. Responsabilidade Civil no comércio B2C (Business to Consumer). **Revista de Direito Empresarial**, v. 18, p. 99 – 119. set, 2016.

CELLA, José Renato Gaziero; DONEDA, Danilo Cesar Maganhoto. Lógica, inteligência artificial e comércio eletrônico. *In*: CONGRESSO NACIONAL DO CONPEDI, 18., São Paulo. **Anais** [...]. São Paulo, 2009.

CORRÊA, Leonardo. Um paradoxo da Lei Geral de Proteção de Dados. **Revista Consultor Jurídico**, 2019. Disponível em: https://www.conjur.com.br/2019-jan-04/leonardo-correa-paradoxo-lei-geral-protecao-dados. Acesso em: 22 maio 2019.

DONEDA, Danilo; MENDES, Laura Schertel. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, v 120. São Paulo: Ed. RT, 2018.

DONGPO, Zang. Big Data Security and Privacy Protection. **Advances in Computer Science Research.** v.77, p. 275-278, 2018.

FRAZÃO, Ana. **A nova Lei geral de Proteção de Dados:** repercussões para a atividade empresarial: o alcance da LGPD**.** São Paulo. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-emercado/o-alcance-da-lgpd-e-repercussoes-para-a-atividade-empresarial05092018. Acesso em: 13 abr. 2018.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo Curso de Direito Civil, volume 1:** parte geral. 17 ed. São Paulo: Saraiva, 2015.

GMACH, Deomar Adriano. Marketplace: contornos jurídicos e a responsabilidade civil nos acidentes de consumo. **Revista dos Tribunais**. v. 995.p.261 – 283.set, 2018.

KLEE, Antonia Espíndola Longoni. O Diálogo das Fontes nos contratos pela internet: do vínculo contratual ao conceito de estabelecimento empresarial virtual e a proteção do consumidor. **Revista de Direito do Consumidor**, v. 77. p. 99 – 150. jan. – mar., 2011.

MARQUES, Cláudia Lima. Confiança no comércio eletrônico e a proteção do consumidor: um estudo dos negócios jurídicos de consumo no comércio eletrônico. **Revista dos Tribunais,** São Paulo, 2004.

MARQUES**,** Cláudia Lima. **Contratos no código de defesa do consumidor**: o novo regime das relações contratuais. 5. ed. São Paulo: Revista dos Tribunais, 2006.

MARQUES, Cláudia Lima. **Contratos no código de defesa do consumidor:** o novo regime das relações contratuais. 8. ed. São Paulo: Revista dos Tribunais, 2016.

MARQUES, Cláudia Lima. Proteção do consumidor no comércio eletrônico e a chamada nova crise do contrato: por um Direito do Consumidor aprofundado. **Revista de Direito do Consumidor**.v.57. p. 9-59. jan – mar, 2006.

MARTINS, Guilherme Magalhães. **Responsabilidade Civil por acidente de consumo na internet**. 2 ed. São Paulo: Ed. Revista dos Tribunais, 2014.

MENDES, Laura Schertel Mendes. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDONÇA, Fernanda Graebin. **O direito à autodeterminação informativa:** a (des)necessidade de criação de um novo direito fundamental para a proteção de dados pessoais no brasil. In: SEMINÁRIO INTERNACIONAL DE DEMANDAS SOCIAIS E POLÍTICAS PÚBLICAS NA SOCIEDADE CONTEMPORÂNEA, 11.- Mostra de Trabalhos Jurídicos Científicos, 7. 2014.

MIRAGEM, Bruno. **Curso de direito do consumidor.** 6ed. São Paulo: Editora Revista dos Tribunais, 2016.

MONTEIRO, Renato Leite. **Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?**. Instituto Igarapé- Artigo estratégico 39. dez., 2018.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/2018). **Revistas de Direitos e Garantias Fundamentais**, v.19.n.13.p.159-180.set. – dez ,2018.

NISSENBAUN, Helen. **Privacy in Context:** Tecnology, Policy and the Integrity of Social Life. Stanford: Stanford University Press, 2010.

OBAR, Jonathan A.; OELDORF-HIRSCH, Anne. **The biggest lie on the internet:Ignoring the privacy policies and terms of services policies of social networking services**.Michigan State University,2016.

OBAR, Jonathan A.; OELDORF-HIRSCH, Anne. The Clickwrap: A Political Economic Mechanism for Manufacturing Consent on Social Media. **Social Media+ Society**. p.1-14. jul-set.,2018.

OLIVEIRA, Ricardo Alexandre de. Lei Geral de Proteção de Dados pessoais e seus impactos no ordenamento jurídico. **Revista dos Tribunais**, v. 998. p. 241 – 261.dez.,2018.

PINHEIRO, Patricia Peck Garrido. **Direito Digital.** 4ed**.** São Paulo: Saraiva, 2010.

PINHEIRO, Patrícia Peck Garrido. Nova Lei Brasileira de Proteção de Dados Pessoais (LGPD) e o impacto nas instituições públicas e privadas. **Revista dos Tribunais**, v. 1000. p. 309 – 323.fev., 2019.

PIRES, Lucas de Almendra Freitas Pires. **Direito à Privacidade no Âmbito da Sociedade da Informação:** reflexões em torno da questão nos inícios do século XXI. Coimbra, 2014.

RODRIGUES, Yuri Gonçalves dos Santos; FERREIRA, Keila Pacheco. A Privacidade no ambiente virtual: avanços e insuficiências da Lei Geral de Proteção de Dados no Brasil (lei 13.709/18). **Revista de Direito do Consumidor,** v. 122. mar.- abr., 2019.

SALDANHA, Jânia Maria Lopez *et al*. As novas Tecnologias da informação entre a promessa de liberdade e o risco de controle total: estudo da jurisprudência do sistema interamericano de direitos humanos. Universidade Nacional Autónoma de México. Instituto de Investigaciones Jurídicas. **Anuário Mexicano de Derecho Internacional.** v. 16. p. 491-498. 2016.

SANTOS, Fabíola de Almeida; TALIBA, Rita. Lei geral de Proteção de Dados no Brasil e os possíveis impactos. **Revista dos Tribunais**. v. 998. p. 225 – 239. dez., 2018.

SANTOS; Thiago de Oliveira dos; DUARTE, Bruno Ferreira Montenegro. A Responsabilidade Civil dos Provedores de Aplicação de Internet no Tratamento de Dados à luz da Lei n.º 12.965/2014 denominada Marco Civil da Internet. **Revista de Direito da Faculdade Estácio do Pará**. v.5.n.7.p.79- 100. jun.,2018.

SARAIVA NETO, Pery; FENILI, Maiara Bonetti. Novos marcos legais sobre a proteção de dados pessoais e seus impactos na utilização e tratamento de dados para fins comerciais. **Revista de Estudos Jurídicos e Sociais.** v. 1, n.1, dez.,2018. Disponível em: https://www.univel.br/ojs-3.0.2/index.php/revista/article/view/46. Acesso em: 10 mar. 2019.

SCHREIBER, Anderson. Contratos eletrônicos e consumo. **Revista Brasileira de Direito Civil**. v. 1. jul.-set.,2014.

SENADO NOTÍCIAS. **MP que cria a Autoridade Nacional de Proteção de Dados ainda aguarda instalação de Comissão Mista.** Brasília, 2019. Disponível em: https://www12.senado.leg.br/noticias/materias/2019/03/12/mp-que-cria-a-autoridade-nacional-de-protecao-de-dados-ainda-aguarda-instalacao-de-comissao-mista. Acesso em: 20 maio 2019.

SILVA, Joseane Suzart da. A Proteção de Dados pessoais dos consumidores e a lei 13.709/2018: em busca da efetividade dos direitos a privacidade, intimidade e autodeterminação**. Revista de Direito do Consumidor**, v. 121, p. 367 – 418, 2019**.**

SILVA, Michael César; SANTOS, Wellington Fonseca. O direito do consumidor nas relações de consumo virtuais**. Revista de Informação Legislativa**, v.49, n. 194, abr.- jun., 2012.

SOARES, Dennis Verbicaro; VERBICARO, Loiane da Ponte Souza Prado. A indústria cultural e o caráter fictício da individualidade na definição de consumidor-comunidade global. **Revista jurídica Cesumar**, v.17, n1. p.107-131. jan.-abr., 2017.

SOUSA, Jéffson Menezes de. **A efetividade da proteção de dados pessoais frente ao BIG DATA.** Aracaju. 2017.

SOUZA, Thiago Pinheiro Vieira de. **A proteção de dados pessoais como direito fundamental e a (in)civilidade dos *cookies***. Uberlândia, 2018.

UOL.**500 milhões de clientes da rede de hotéis Marriott podem ter sido hackeados**. São Paulo. 2018. Disponível em: https://noticias.uol.com.br/tecnologia/noticias/afp/2018/11/30/500-milhoes-de-clientes-da-rede-de-hoteis-marriott-podem-ter-sido-hackeados.htm. Acesso em: 01 dez. 2018.

VERBICARO, Dennis; MARTINS, Ana Paula Pereira. A contratação eletrônica de aplicativos virtuais no Brasil e a nova dimensão da privacidade do consumidor. **Revista de Direito do Consumidor**. v 116. ano 27. p. 369-391. São Paulo: Ed. RT, mar.-abr.,2018.

VIAL, Sophia Martini. A sociedade da (des)informação e os contratos de comércio eletrônico: Do Código Civil às atualizações do Código de Defesa do Consumidor, um necessário diálogo entre fontes. **Revista de Direito do Consumidor**. v.88. p.229-257.São Paulo: Ed. RT, jul.-ago.,2013. Disponível em: http://www.sophia.adv.br/artigos/. Acesso em: 12 mar 2019.