

PRIVACIDADE E ECONOMIA DA INFORMAÇÃO: A PROTEÇÃO JURÍDICA BRASILEIRA AOS DADOS PESSOAIS NO AMBIENTE DIGITAL

MONTEIRO, Kerin Costa¹
AGUERA, Thayara Garcia Bassegio²

RESUMO:

É inegável a mudança do paradigma apresentado pela sociedade contemporânea. Há que se pontuar que o capitalismo do século XXI apresentou uma nova forma de desenvolvimento econômico em que a informação é um elemento lucrativo quando se convertem em informações necessárias para atividade econômica. O fato é que com esta facilidade de acesso houve o aumento exponencial da produção de dados, ocasionando diversos questionamentos sobre privacidade, comercialização e consentimento de uso de dados pessoais. Diante dessa necessidade de proteger a extração e uso dos dados, foi promulgada a Lei 13.709/2018, Lei Geral de Proteção de Dados – LGPD que regula o tratamento de dados pessoais, visando à proteção das pessoas durante a interação digital, em contrapartida, em seu artigo 2º, inciso II, há o direito à autodeterminação dos dados e informações pessoais. Nesse sentido, este trabalho pretende esclarecer, por meio dos dispositivos legais e estudiosos da área, em que medida a aplicação da Lei Geral de Proteção de Dados protege de maneira efetiva os dados pessoais, mais especificamente quanto à privacidade, extração, comercialização e utilização. Por outro lado, existe a responsabilidade do Estado em proteger este direito fundamental, à adequada e efetiva proteção dos dados sensíveis dos cidadãos, da sua privacidade e da autodeterminação em relação aos seus dados pessoais de forma expressa, elementos que constituem um direito mais amplo da dignidade e da personalidade humana.

PALAVRAS-CHAVE: Direito à privacidade, Proteção de dados sensíveis, Autodeterminação informativa.

PRIVACY AND INFORMATION ECONOMY: BRAZILIAN LEGAL PROTECTION TO PERSONAL DATA IN THE DIGITAL ENVIRONMENT

ABSTRACT:

The paradigm shift presented by contemporary society is undeniable. It is necessary to punctuate the capitalism of the 21st century presented a new form of economic development in which information is a profitable element when it becomes information necessary for economic activity. The fact is that with this ease of access there was an exponential increase in data production, causing several questions about privacy, marketing and consent to the use of personal data. Faced with this need to protect the extraction and use of data, Law 13.709/2018, General Data Protection Law – LGPD that regulates the processing of personal data, aimed at the protection of people during digital interaction, in contrast, in article 2, item II, there is the right to self-determination of personal data and information. In this sense, this work intends to clarify, through the legal and scholarly provisions of the area, to what extent the application of the General Data Protection Law effectively protects personal data, more specifically regarding privacy, extraction, marketing and use. On the other hand, there is the responsibility of the State to protect this fundamental right, the proper and effective protection of citizens' sensitive data, their privacy and self-determination in relation to their personal data in an express way, elements that constitute a broader right of dignity and human personality.

KEYWORDS: Right to privacy, Protection of confidential data, Informational self-determination.

¹Acadêmica do 9º período do Curso de Direito do Centro Universitário FAG. E-mail: monteirokerin@gmail.com

²Docente orientadora do curso de Direito do Centro Universitário FAG. E-mail: thayarabassegio@fag.edu.br

1 INTRODUÇÃO

O assunto deste trabalho está pautado no Direito Digital. O tema norteador é a proteção jurídica dos dados pessoais deixados durante as interações digitais sob a ótica da privacidade e economia da informação.

O capitalismo do século XXI trouxe consigo um marco na história da humanidade: a expansão do uso da internet por meio das interações digitais. O fato é que com esta facilidade de acesso houve o aumento exponencial da produção de dados, ocasionando diversos questionamentos sobre privacidade, comercialização e consentimento de uso de dados pessoais.

Consequentemente, todo esse fluxo gerado por nossas informações pessoais está, em tese, sendo inserido de forma ‘personalíssima’ por cada indivíduo no decorrer da vida, passando a fazer parte do patrimônio deste indivíduo.

É verdade que a coleta desses dados não é algo atual, pois, há pelo menos uma década, eram colhidos de forma somente quantitativa, no entanto, após o surgimento do *Big data*, eles tornaram-se valiosos, gerando informações completamente novas a partir da combinação dos dados e da análise em conjunto sendo utilizadas para a elaboração de ações estratégicas.

Entretanto, ainda que não se consiga prever a extensão do poder econômico, político e social decorrente dos dados e de seu uso, é possível prever o quão grande e lucrativo ele pode ser quando se convertem em informações necessárias para atividade econômica.

Diante dessa necessidade de proteger a extração e uso dos dados, foi promulgada a Lei 13.709/2018, Lei Geral de Proteção de Dados – LGPD que regula o tratamento de dados pessoais, visando à proteção das pessoas durante a interação digital, em contrapartida, em seu artigo 2º, inciso II, há o direito à autodeterminação dos dados e informações pessoais com fundamento da supracitada legislação.

Complementando a proteção jurídica no âmbito da privacidade, dispõe a Carta Magna de 1988, no seu artigo 5º, incisos X e XII, que é direito fundamental garantir a inviolabilidade e o sigilo das informações, da intimidade e da vida privada, da honra e da imagem de todos os cidadãos, podendo haver exceção, em último caso, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

Nesse sentido, cabe ao Estado a adequada e efetiva proteção dos dados sensíveis dos cidadãos, da sua privacidade e da autodeterminação em relação aos seus dados pessoais de forma expressa, elementos que constituem um direito mais amplo da dignidade e da personalidade humana.

Este trabalho tem o objetivo de esclarecer, por meio dos dispositivos legais e estudiosos da área, em que medida a aplicação da Lei Geral de Proteção de Dados protege de maneira efetiva os dados pessoais, mais especificamente quanto à privacidade, extração, comercialização e utilização.

Dito isso, registra-se que este tema já foi levado para votação ao Supremo Tribunal Federal por meio de Ações Diretas de Inconstitucionalidade – ADIs, ajuizadas contra a Medida Provisória – MP 954/2020. O argumento comum é que os dados disponibilizados contêm nomes, números de telefone e dos endereços de seus consumidores, violando os dispositivos da Constituição Federal que asseguram a dignidade da pessoa humana, a inviolabilidade da intimidade, da vida privada e do sigilo dos dados.

Deve-se salientar que o tema proposto no projeto de pesquisa necessita de uma leitura contemporânea. Dessa maneira, observa-se que o tema apresentado é de grande relevância para os cidadãos, visto que existe a responsabilidade do Estado em proteger este direito fundamental.

Após concluso, o projeto deverá ser instrumento norteador para promover segurança jurídica em decisões que versam sobre este tema no país, bem como propiciar o conhecimento para acadêmicos, advogados e juristas desta área de pesquisa.

2 COLETA DE DADOS PESSOAIS E A PRIVACIDADE NO AMBIENTE VIRTUAL

No século passado, quando havia a necessidade de comunicar-se ao redor do mundo, eram utilizadas ligações telefônicas ou correspondências; porém, na era digital, o panorama é outro, porque a internet revolucionou a comunicação e apresentou uma nova maneira de conectar-se de forma instantânea.

É inegável a mudança deste paradigma apresentado pela sociedade contemporânea. Há que se pontuar uma nova forma de desenvolvimento econômico em que a informação é o elemento estruturante e organizador da sociedade, fortalecida pelo avanço tecnológico com um fluxo informacional que não encontra mais obstáculos físicos e de distância (FRAZÃO, 2019).

Cada vez mais os usuários da Internet tornam-se consumidores, sendo possível notar esse fato com o aumento das vendas online, da utilização das mídias sociais, no crescimento de sites para empresas e o fluxo de dados, notados através dos *cookies*, no qual é possível rastrear a navegação do usuário e inferir seus interesses e, dessa maneira, ofertar o produto com um alto grau de personalização a este comprador (FRAZÃO, 2019).

Não obstante, para além de identificar hábitos de navegação pelo computador, soma-se a indústria de telefones celulares que permitiu aos usuários ficar durante vinte e quatro horas na internet, gerando uma conexão exata nos ambientes online e off-line, permitindo aos aplicativos que possuem *GPS – global positioning system* a mapear sua localização geográfica, como é o caso dos aplicativos *WAZE* ou *GOOGLE MAPS* e, prontamente, oferecer serviços ou produtos nas proximidades da sua viagem ou do seu passeio (TEPEDINO *et al*, 2019).

Nesse cenário de facilidades e entretenimento, as ligações telefônicas foram substituídas pelo *Whatsapp* com textos, áudios e *emoticons*; qualquer música, livro ou série estão ao alcance em apenas um clique e de forma personalizada, em todo esse contexto, estamos emitindo reações emocionais em forma de dados para uma indústria faminta instigar o consumo, numa coleta de dados contínua (TEPEDINO *et al*, 2019).

De fato, a grande porcentagem destes serviços online oferecidos por meio dos aplicativos não necessita de uma contraprestação pecuniária para utilização dos usuários, como por exemplo, os e-mails, buscadores de informações, portais de notícias, mídias sociais. Trata-se de uma relação plurilateral, na qual o consumidor pode utilizar o serviço ao passo que aceita compartilhar seus dados pessoais com a empresa e esta, por vez, os cedem para publicidade, movimentando um ciclo econômico (TEPEDINO *et al*, 2019).

Não por outro motivo, Bioni (2019) retrata a importância da informação no mercado econômico, apresentando a eficácia dos dados extraídos junto ao público consumidor em uma das maiores redes de varejo do mundo, a Zara, os bens de consumo são projetados conforme a necessidade do consumidor, sendo este o conhecimento gerado dos dados extraídos das vendas junto ao seu público-alvo.

E ainda, nesse sentido, as informações colhidas acerca dos hábitos de consumo dos cidadãos permitem empreender de forma mais eficiente no mercado, aumentando o sucesso dos produtos junto aos compradores, quer seja melhorando o design, a segmentação ou o marketing com intuito de vender mais (BIONI, 2019).

Complementa o autor que, com a possibilidade de escalar, organizar e utilizar tais dados por meio do *Big Data*, criou-se um mercado de *commodities* de dados, que não se restringe somente à economia, mas também ao âmbito social e político. O capitalismo gera uma espécie de ‘observação’ sobre informações pessoais mais íntimas e emoções, imagens e vozes, entretanto, quando se adentra à esfera da personalidade e privacidade individual do usuário, pode causar diversas controvérsias jurídicas (TEPEDINO *et al*, 2019).

Para tanto, faz-se uma análise por meio do termo sociedade de vigilância, em que tais agências sabem tudo sobre o cidadão de forma barata, automática e às escuras. Porém, quando

essa violação torna-se um negócio lucrativo, fomentado pela monetização de dados, possibilita a acumulação de um grande poder que se retroalimenta indefinidamente (TEPEDINO *et al*, 2019).

A grande questão é que essa estratégia compromete a liberdade de uso e difusão de informação dentro da internet, colocando em risco os direitos individuais e o próprio crescimento econômico. Todo esse ciclo promovido pela vivência diária dos usuários no ambiente virtual fez emergir uma grande preocupação social em proteger a privacidade dos seus dados pessoais, fazendo com que o Estado e o Direito se desenvolvessem de forma a encontrar soluções de proteção jurídica para os cidadãos (CARVALHO, 2018).

Por isso da importância da LGPD – Lei Geral de Proteção de Dados para que o Estado promova a proteção dos dados pessoais a fim de evitar que sejam utilizados para formação de perfis ou grupos comportamentais, conforme disposto no artigo 12, §2, o foco são as consequências que este tratamento de dados indevido não anonimizado possa causar na esfera do indivíduo (BIONI, 2019).

Nesse sentido, a proteção dos dados pessoais está inserida aos direitos da personalidade, principalmente quando se trata dos dados sensíveis, pois relaciona a pessoa a uma condição de vulnerabilidade e/ou discriminação, tais como: orientação religiosa, sexual, política e racial, estado de saúde, filiação sindical (BIONI, 2019).

Exemplos não faltam, como o de uma loja de departamentos americana que identificou quais consumidoras estariam grávidas e qual mês de gestação, ou, ainda, um estudo universitário inglês que criou um retrato fiel das ‘curtidas’ de uma rede social, mostrando com exatidão quantos eram homossexuais, brancos ou negros e, destes, quais eram republicanos ou democratas (BIONI, 2019).

Do outro lado, não se pode deixar de notar que o protagonismo dos dados mantém-se no consentimento do usuário e a legislação tem focado neste ponto para nortear sua proteção jurídica, uma espécie de autodeterminação informacional expressa por meio de contratos de adesão proposto ao adentrar as ferramentas digitais ou a aceitação do compartilhamento de dados ao comprar um produto online (TEPEDINO *et al*, 2019).

Por fim, a proteção dos dados pessoais sobrepõe ao princípio da isonomia tornando um instrumento de controle de práticas discriminatórias, propondo um regime jurídico protetivo em relação aos dados mais sensíveis com a finalidade de que o indivíduo possa desenvolver livremente sua personalidade e relacionar-se perante a sociedade sem sofrer preconceitos e por outro lado a autonomia informativa (BIONI, 2019).

3 EVOLUÇÃO LEGISLATIVA SOBRE PRIVACIDADE E PROTEÇÃO DE DADOS

Falar sobre o termo privacidade dentro do Direito não é tarefa fácil, pois engloba uma quantidade de legislações, diversas tutelas e a falta de uma conceituação concreta sobre o tema dentro do ordenamento jurídico. Para ficar mais claro o tema, cabe compreender o arcabouço legal e a histórica que fortaleceu a privacidade até os dias atuais.

Dito isso, ainda que brevemente, é importante abordar o trajeto histórico sobre a consolidação da privacidade, com intuito de observar como foi inserida dentro do sistema jurídico para depois tratar junto à proteção dos dados pessoais (BIONI, 2019).

Neste trecho de seu artigo, Carvalho (2018) descreve que os direitos da personalidade são tratados de acordo com a perspectiva do ser humano, como se observa, diferentemente de outras culturas jurídico-legais anteriores (e.g., Código de Hamurabi) que baseavam a tutela da pessoa humana tão somente na tutela da integridade física. Também, passou-se a situá-los no campo moral (e.g., tutela da honra), a ideia de uma ciência jurídica que o homem teria direitos que lhe seriam inatos e decorrentes da sua própria natureza humana.

Nesse caminho, a pessoa humana perdeu seu espaço para excessiva preocupação com o patrimônio, somando-se a isso, era negado o direito de reconhecer os direitos da personalidade porque não existia norma positivada (CARVALHO, 2018).

Foi então, após a segunda guerra mundial, que a privacidade é posta em um tratado, conforme relata Carvalho (2018, p. 41), “Declaração Universal dos Direitos do Homem”, de 1948, que previu em seu art. XII a proteção dos indivíduos contra ‘ingerências arbitrárias em sua vida privada’”. Há que se destacar que, no Brasil, a proteção legislativa sob o crivo da pessoa humana perpassou durante décadas, sendo apreciada durante a criação do Código Civil de Orlando Gomes, promovendo maior proteção à pessoa quanto aos direitos da personalidade.

Muito embora já existisse a visão negocial sobre a pessoa dentro da legislação civilista, somente com a promulgação da Constituição Federal de 1988 é que foi incluída entre as garantias fundamentais, em seu artigo 5º, inciso X, a proteção à intimidade e vida privada e sigilo de comunicações:

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
X – São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação;
XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

Com foco na legislação apontada e no liame histórico, vale inferir que a função dos direitos da personalidade, leia-se direito à privacidade, é assegurar a proteção à pessoa humana no que se refere ao acesso à informação personalíssima produzida em ambiente digital, e, para isso, faz-se necessário criar uma relação entre as novas tecnologias e o direito. Sob a perspectiva da interpretação jurídica, os dados pessoais têm aspecto de personificação, assim como nome, voz, imagem (BIONI, 2019).

É importante ressaltar que, com o desenvolvimento das interações digitais, foram aparecendo novos problemas em relação ao direito à privacidade, demandando novas respostas e soluções na tutela deste aspecto da pessoa, tornando, se não obsoletas, talvez incompletas as soluções anteriormente alcançadas pelo Direito (BIONI, 2019).

Dessa feita, faz-se necessário voltar no contexto histórico em que surgiram as primeiras leis de proteção de dados pessoais no mundo para compreender como chegou no sistema legislativo atual. A primeira geração de leis surgiu na formação do Estado Moderno, com foco na esfera do governo; a segunda geração foi caracterizada pela preocupação em proteger dados públicos e privados, aqui transfere para o próprio titular dos dados a responsabilidade de protegê-los (PINHEIRO, 2018).

Consequentemente, na terceira geração, o titular tinha o poder da autodeterminação informacional. Nesta fase, é possível relatar a decisão da Corte Constitucional Alemã, pois o julgado determina deveres para quem coleta e processa os dados pessoais minimizando o poder do titular dos dados; a quarta e última geração veio para corrigir as falhas que haviam nas legislações anteriores. Entretanto, o titular continuou como foco na abordagem regulatória, criou a possibilidade de autoridades independentes aplicarem a lei e tirou o poder do titular de ceder seus dados sensíveis, relativizando em partes seu poder sobre as informações (BIONI, 2019).

Após esse primeiro panorama, na década de 1980, a OCDE – Organização para o Desenvolvimento e Cooperação Econômica propôs diretrizes para o desenvolvimento econômico por meio dos dados pessoais, ou seja, direitos e obrigações para o cidadão, para a empresa privada e para o governo, de como deveria ser processados os dados pessoais ao redor do mundo; emitiu ainda as *guidelines*, normas sobre proteção de dados pessoais para os países-membros com intuito de livre informação entre eles e *declaration on transborder data flows em 1985*, ou seja, fluxo de dados além das fronteiras dos Estados-membros (PINHEIRO, 2018).

Em decorrência desse fato, houve, em 2015, a regulação da diretiva de proteção de dados no direito comunitário europeu, GDPR - *General Data Protection Regulation*, que manteve a

decisão no foco do titular de dados e deixou claro que o processo de aceitação de dados pelo possuidor deveria ser feito de maneira transparente e de fácil compreensão (PINHEIRO, 2018).

Esse aspecto é de fundamental importância para compreender como surgiram as leis de proteção de dados no Brasil. Diante disso, importa apresentar as legislações que tutelam este direito ante tal contextualização (TEPEDINO *et al*, 2019).

Lei 12.572/2011, Lei de Acesso à Informação, dispõe que os arquivos cuja divulgação violasse a intimidade ou a vida privada, assim como ameaçasse a segurança da sociedade, eram considerados sigilosos e, portanto, submetidos a regras especiais (TEPEDINO *et al*, 2019).

Lei 8.078/1990, Código de Defesa do Consumidor, possui uma seção dedicada ao banco de dados do consumidor, dispõe o artigo 43:

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

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

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

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

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

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

§ 6º Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor.

Lei 12.414/2011, Lei do Cadastro Positivo dispõe a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito; a iniciativa é permitir que o mercado identifique os bons pagadores e, com isso, reduza a taxa de juros, sem descuidar, porém, da proteção dos dados pessoais, inclusive as informações sensíveis,

Lei 12. 965/2014, Marco Civil da Internet, trata em seu artigo 3º, inciso III, elegendo-o como um princípio do uso da internet no Brasil:

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

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

II - Proteção da privacidade;

III - proteção dos dados pessoais, na forma da lei;
 IV - Preservação e garantia da neutralidade de rede;
 V - Preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
 VI - Responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
 VII - preservação da natureza participativa da rede;
 VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
 Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Ainda, em continuidade à Lei 12. 965/2014, complementa que no artigo 11, assegura a aplicação da legislação brasileira para proteção dos dados quando ao menos uma das atividades de tratamento seja realizada no Brasil (TEPEDINO *et al*, 2019).

Ao observar as legislações descritas até o momento, apesar das inegáveis contribuições para que os cidadãos tivessem os direitos à proteção dos dados pessoais materializados, foram incapazes de atender às múltiplas situações de tutela e possível violação deste direito. Entretanto, há que frisar que a Lei 13.709/2018, LGPD - Lei Geral de Proteção de Dados, após uma década de debates, foi criada para abarcar esse vácuo legislativo (CARVALHO, 2018).

4 LGPD: PRINCIPAIS ASPECTOS SOBRE A LEGISLAÇÃO

A principal motivação para criar uma regulamentação da proteção de dados pessoais consolidou-se nos anos de 1990, e foi fortalecida pela globalização e está intrinsecamente ligada aos novos modelos de negócios digitais e a internacionalização de empresas e consequentes crises tecnológicas que viessem causar danos aos consumidores.

Décadas depois, em 27 de abril de 2016, foi promulgada a GDPR – Regulamento Geral de proteção de Dados Europeus nº 679, que tinha como finalidade a proteção de dados de pessoas físicas e a livre circulação destas, sendo que permitia um prazo de dois anos para aplicação de sanções a quem violasse esta legislação (PINHEIRO, 2018).

Por sua vez, todos os países que mantivessem relações econômicas com a União Europeia deveriam promover uma legislação que possuísse mesmo nível de proteção ou haveria dificuldades em fazer negócios com o bloco econômico, visto que há uma busca por harmonizar os negócios digitais sem fronteiras (PINHEIRO, 2018).

Com essa motivação, foi promulgada a Lei 13.709/2018, em 14 de agosto de 2018 e com vigência a partir de agosto de 2020, conhecida como Lei Geral de Proteção de Dados –

LGPD, desenvolvida com o objetivo de proteger os titulares dos dados e seus direitos básicos em relação à autodeterminação informativa. Esta novidade legislativa trará impacto significativo para as empresas que terão de ajustar suas atividades à lei (TEPEDINO *et al*, 2019).

Sua criação promove o consentimento livre, informado, inequívoco, com uma finalidade determinada e específica, segue toda a evolução do direito comunitário europeu e da quarta geração de leis de proteção de dados pessoais e porque todos os princípios são focados no indivíduo, quem tem o controle dos dados nas mãos (BIONI, 2019).

Dessa forma, em síntese, há que observar a aplicação dos princípios, propósitos e valores principais, sendo o foco e proteção dos direitos fundamentais, liberdade e privacidade, conforme relatado nos artigos 1º e 2º. Com efeito, temos o artigo 5º, inciso I, que regula qualquer informação de uma pessoa que seja identificada ou identificável; inciso V, somente poderão ser manipuladas pelos setores públicos ou privados por meio de autorização; já conforme inciso X, toda operação realizada com dados pessoais e o artigo 6º os princípios norteadores da legislação: boa-fé objetiva, princípios da finalidade, da adequação, mínimo necessário, livre acesso, qualidade dos dados, transparência, segurança, prevenção e não discriminação; todo e qualquer tratamento de dados deve respeitar a base legal definida no artigo 7º (TEPEDINO *et al*, 2019).

Convém deixar claro que o conteúdo legislativo aplica-se a todos que façam o tratamento de dados pessoais, sejam eles órgãos públicos ou privados, pessoas jurídicas ou físicas, desde que ocorra “(i) em território nacional; (ii) que tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; (iii) em que os dados tenham sido coletados no território nacional” (PINHEIRO, 2018. p.22).

No entanto, quando se trata de negócios digitais sem fronteiras, é importante ressaltar os efeitos internacionais, na medida em que se aplica também aos dados que sejam tratados fora do Brasil, desde que a coleta tenha ocorrido em território nacional, ou por oferta de produto ou serviço para indivíduos no território nacional ou que estivessem no Brasil. Assim, o dado pessoal tratado por uma empresa de serviço de armazenamento de dados fora do país, terá que cumprir as exigências da LGPD (PINHEIRO, 2018).

No tocante às sanções apresentadas, apesar da exclusão de alguns vetos para reduzir, mantiveram-se as seguintes: advertência com prazo de correção, multa simples de 2% do faturamento da pessoa jurídica, grupo ou conglomerado, no piso máximo de R\$ 50 milhões de reais por cada infração, multa diária, publicização da infração depois de confirmada a

ocorrência, bloqueio dos dados pessoais violados até a regularização ou eliminação destes (PINHEIRO, 2018).

Em que pese a LGPD, o tema teria sido bem mais abrangente e eficaz em sede de Tratado Internacional, visto que os negócios digitais são em sua maioria sem fronteiras, como exemplo:

Apenas a título ilustrativo, uma instituição brasileira que capture dados no Brasil, em território nacional, mas que tenha um aplicativo que permita que o cliente seja de qualquer cidadania, nacionalidade, residência, e, portanto, o usuário do serviço, titular dos dados, pode ser um europeu, que mantém sua vida em um país da União Europeia, mas está temporariamente a trabalho no Brasil, utiliza cartão de crédito internacional, acaba por atrair, em termos de aplicação de leis e jurisdição para a sua operação, tanto a regulamentação nacional (LGPD) como também a regulamentação europeia (GDPR). Se essa instituição brasileira utilizar recursos na nuvem e fizer a guarda internacional dos dados pessoais em outro país, poderá atrair ainda outras regulamentações (como o *Cloud Act*, dos EUA) (PINHEIRO, 2018, p. 28).

Daí a importância de observar como é complexo implementar esta regulamentação neste panorama digital internacional, devendo ainda observar a possibilidade de aplicação do Direito Comparado e Direito Internacional em casos concretos (PINHEIRO, 2018).

Sob essa perspectiva legislativa, o que está sendo tratado diz respeito à privacidade no sentido da intimidade e da autonomia informativa e o controle sobre a informação da pessoa natural, considerando que as bases da democracia hoje dependem da regulação de dados (TEPEDINO *et al*, 2019).

Na sequência serão expostas e analisadas as opiniões de estudiosos acerca do tema tratado neste projeto de pesquisa, apresentadas opiniões positivas e negativas quanto à proteção do Estado sobre os dados dos cidadãos frente às grandes empresas e a própria máquina estatal.

Couto e Cassio (2018) concluem, em seu estudo, que conforme a LGPD, o Estado, mediante entes da administração pública, tem normas de conduta a serem seguidas e aplicadas em relação ao uso e manuseio de dados pessoais para proteção do cidadão hipossuficiente em face ao autoritarismo estatal ou das grandes corporações. Ademais, torna o ordenamento jurídico mais contemporâneo quando se trata de assuntos em ambiente digital, ainda que existam possibilidades de ‘interpretações’ jurídicas quanto ao tema.

Por sua vez, Pontes (2018) afirma, em seu artigo, que o grande objetivo da LGPD é estabelecer regras para o Estado e empresas tratarem os dados pessoais e fixarem limites para que problemas como comercialização de dados não ocorram. Dessa forma, o Estado tem a função de regular os dados e quem os utiliza, podendo ser passível de multa ações irregulares que órgãos ou empresas pratiquem.

Nas palavras de Carvalho (2018), a LGPD estabeleceu que, em operações de coleta, armazenamento e tratamento de dados pessoais, desde que pelo menos uma das fases ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. É essencial a presença do Estado frente a este tema em razão dos riscos que essa atividade apresenta em relação aos direitos fundamentais dos sujeitos de direito.

Quando se trata de opinião desfavorável quanto à proteção de dados pessoais pelo Estado, foi encontrado apenas uma tese contrária, trata-se da autodeterminação dos dados pessoais, ou seja, o indivíduo, por direito, deve ter controle ou transparência sobre a destinação de seus dados.

Nesse âmbito do consentimento, por meio das políticas de privacidade ilegíveis nos contratos de adesão, o mercado colhe e comercializa todos os dados que detém sob seu poder, sem controle governamental (BIONI, 2019).

Entretanto, a partir de 1983, em julgamento no Tribunal Constitucional Alemão, iniciou-se uma nova fase na proteção dos dados, e, com isso, foi constatado que não existem mais dados insignificantes e o consentimento foi relativizado (BIONI, 2019).

No Brasil, o STF manteve uma decisão histórica ao reconhecer que a Constituição Federal/88 assegura aos cidadãos o direito à autodeterminação informativa, devendo o uso dos dados e informações pessoais ser controlado pelo próprio indivíduo, exceto quando a legislação estritamente determinar (COELHO, 2020).

Sendo os dados o maior ativo do último século, cabe ao Estado proteger apenas àqueles mais sensíveis do cidadão e a este manifestar seu poder de autodeterminação sobre seus dados pessoais, embasados pelos direitos e garantias jurídicas que nos protegem de acordo com as mudanças sociais (COELHO, 2020).

Por fim, deve-se compreender dados sensíveis àqueles que se referem a crianças e adolescentes e que revelam convicções filosóficas ou de religião, raça ou etnia, opiniões políticas, filiação sindical, questões sobre genética, biométrica, saúde e vida sexual do indivíduo (COELHO, 2020).

5 JULGADOS RECENTES COM DECISÕES EMBASADAS NA LGPD

A intenção do legislador ao criar a LGPD foi de proteger a privacidade e os direitos fundamentais embasados nos princípios e nas premissas dos direitos humanos contribuindo para

que seja um ambiente seguro e com vistas ao progresso social e econômico. Diante disso, cabe apresentar as mais recentes decisões levadas a instâncias superiores após entrada em vigor da supracitada lei.

Sob essa perspectiva de proteção à privacidade, a liminar da 17ª Vara Cível de Brasília referente ao processo 0733785-39.2020.8.07.0001, determinou que o portal Mercado Livre suspenda o anúncio da venda dos dados e forneça os dados cadastrais do usuário da plataforma nominado EMARKETING011ERICAVIRTUAL; este vendia cadastros de brasileiros para uma empresa do Rio Grande do Sul – RS e com a decisão deve se abster de disponibilizar de forma gratuita ou onerosa, sob pena de multa de R\$ 2 mil reais para cada operação (TJDFT, 2020).

O Ministério Público do Distrito Federal argumenta que a prática ofende a privacidade daqueles cujos dados são comercializados e o magistrado observou, em sua decisão, que a empresa comercializa dados identificáveis e não há indícios que os titulares dos dados concordem com a venda, violando a Constituição Federal e LGPD (TJDFT, 2020).

Por sua vez, foi deferida a Tutela Provisória em Ação Civil Pública 0733646-87.2020.8.07.0001, promovida pelo Ministério Público do Distrito Federal contra o site www.facilitavirtual.com.br que comercializava informações pessoais como nomes, e-mails, contatos para SMS, bairro, Cidade, Estado e CEP de usuários; a decisão é que até segunda ordem deste Juízo não receba qualquer dado ou movimentação, sob pena de multa de R\$ 15.000,00 por cada alimentação/movimentação comprovadamente feita após a intimação desta decisão (TJDFT, 2020).

A decisão da juíza foi pautada no artigo 5, inciso I, e artigo 44, da Lei 13.709/2018, em que as provas revelam a comercialização de dados sem conhecimento dos titulares e também nos princípios de privacidade, consentimento e inviolabilidade dos dados (TJDFT, 2020).

Em sede de Tribunal, uma discussão foi levada ao Superior Tribunal Federal – STF, por meio de Ações Diretas de Inconstitucionalidade – ADIs, propostas pelo Conselho Federal da Ordem dos Advogados do Brasil – OAB (ADI 6387), pelo Partido da Social Democracia Brasileira - PSDB (ADI 6388), pelo Partido Socialista Brasileiro – PSB (ADI 6389), pelo Partido Socialismo e Liberdade – PSOL (ADI 6390) e pelo Partido Comunista do Brasil (ADI 6393) (STF JUS, 2020).

As medidas foram ajuizadas contra a Medida Provisória - MP 954/2020, que prevê o compartilhamento de dados de usuários de telecomunicações com o Instituto Brasileiro de Geografia e Estatística – IBGE para serem utilizados na produção de estatística oficial durante a pandemia do novo coronavírus (STF JUS, 2020).

Entretanto, a Ministra Rosa Weber concluiu seu voto sob o argumento de que os dados disponibilizados contêm nomes, números de telefone e endereços de seus consumidores, violando os dispositivos da Constituição Federal que asseguram a dignidade da pessoa humana, a inviolabilidade da intimidade, da vida privada e do sigilo dos dados (STF JUS, 2020).

Sua decisão acerca do tema vai além a de não definir apropriadamente como e para que serão utilizados os dados coletados, pois a norma não oferece condições para a avaliação da sua adequação e necessidade. Ainda, pode-se afirmar que ela não é capaz de oferecer ferramentas para proteger os dados pessoais de acessos não autorizados, vazamentos acidentais ou utilização indevida. Dessa feita, o STF decidiu manter a suspensão da Medida Provisória - MP 954/2020 (STF JUS, 2020).

6 CONSIDERAÇÕES FINAIS

Levando em consideração os aspectos apresentados, é inegável que a mudança do paradigma decorrente do capitalismo contemporâneo fez com que as informações colhidas em ambiente digital por meio dos dados pessoais se tornassem lucrativas quando convertidas em informações necessárias para atividade econômica.

A grande questão é que essa estratégia compromete a liberdade de uso e difusão de informação dentro da internet, colocando em risco os direitos individuais e o próprio crescimento econômico. Todo esse ciclo promovido pela vivência diária dos usuários no ambiente virtual fez emergir uma grande preocupação social em proteger a privacidade dos seus dados pessoais, fazendo com que o Estado e o Direito se desenvolvessem de forma a encontrar soluções de proteção jurídica para os cidadãos.

Apesar da proteção constitucional e legislações esparsas, não foi possível controlar diversas violações à privacidade dos direitos individuais, vislumbrou-se então a promulgação da Lei 13.709/2018, Lei Geral de Proteção de Dados – LGPD que regula o tratamento de dados pessoais, visando proteger a extração e uso dos dados pessoais durante a interação digital, trazendo punição aos que descumprirem o texto legislativo.

Ocorre que o protagonismo dos dados se mantém no consentimento do usuário e a legislação tem focado neste ponto para nortear sua proteção jurídica, uma espécie de autodeterminação informacional expressa por meio de contratos de adesão proposto ao adentrar as ferramentas digitais ou a aceitação do compartilhamento de dados ao comprar um produto online.

Entretanto, a proteção dos dados pessoais sobrepõe ao princípio da isonomia tornando um instrumento de controle de práticas discriminatórias, propondo um regime jurídico protetivo em relação aos dados mais sensíveis com a finalidade de que o indivíduo possa desenvolver livremente sua personalidade e se relacionar perante a sociedade sem sofrer preconceitos.

Por fim, após análise dos julgados já proferidos, da legislação vigente, da opinião dos estudiosos sobre o tema e estudos bibliográficos, somos levados a acreditar que o Estado enfrentará desafios para adequar a nova legislação, o que exigirá maior segurança na coleta e distribuição dos dados, principalmente os dados sensíveis que deveriam ter proteção integral nesta legislação. Isso por que tratam de informações pessoais como: origem racial ou étnica, nacionalidade, convicção religiosa ou política, saúde, filiação a sindicato, dados biométricos, relativos a vida sexual, e todos aqueles que estão intrinsecamente ligados a menores de idade, vinculados a pessoa natural. Por outro lado, há que considerar que o consumidor tem a liberdade em determinar se quer ceder seus dados sempre de forma específica e destacada e para quais finalidades serão utilizados.

REFERÊNCIAS

BRASIL. Constituição Federal de 1988. Promulgada em 05 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 01 out. 2020.

BRASIL. Lei 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm. Acesso em 01 out. 2020

BRASIL. Lei 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em 01 out. 2020

BRASIL. Lei 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm. Acesso em: 01 out. 2020.

BRASIL. Lei 12.414, de 09 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplimento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112414.htm. Acesso em: 01 out. 2020.

BRASIL. **Lei 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/12965.htm. Acesso em: 01 out. 2020.

BRASIL. **Lei 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 01 out. 2020.

BRASIL. **Supremo Tribunal Federal.** Supremo começa a julgar compartilhamento de dados de usuários de telefonia com o IBGE. Brasília, 2020. Disponível em: <https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442823&ori=1>. Acesso em 30 set. 2020.

DISTRITO FEDERAL. **Tribunal de Justiça do Distrito Federal e dos Territórios.** LGPD: Justiça determina que site suspenda anúncio de venda de banco de dados cadastrais. Brasília, 2020. Disponível em: <https://www.tjdft.jus.br/institucional/imprensa/noticias/2020/outubro/justica-determina-que-site-suspenda-anuncio-de-venda-de-banco-de-dados-caadastrais> Acesso em 24 mai. 2021.

DISTRITO FEDERAL. **Tribunal de Justiça do Distrito Federal e dos Territórios.** Decisão judicial determina congelamento de site que vendia dados pessoais. Brasília, 2020. Disponível em: <https://www.tjdft.jus.br/institucional/imprensa/noticias/2020/outubro/decisao-judicial-determina-congelamento-de-site-que-vendia-dados-pessoais>. Acesso em 24 mai. 2021.

BIONI, B. R. **Proteção de dados pessoais: a função e os limites do consentimento.** 1. Ed. Rio de Janeiro: Forense, 2019.

CARVALHO, V. M. B. **O Direito fundamental à privacidade ante a monetização de dados pessoais na internet: apontamentos legais para uma perspectiva regulatória.** Dissertação (Mestrado em Direito) - Universidade Federal do Rio Grande do Norte, Centro de Ciências Sociais Aplicadas. Programa de Pós-Graduação em Direito. Natal: 2018.

COELHO, M. V. F. O direito à proteção de dados e a tutela da autodeterminação informativa. **Revista Consultor Jurídico**, jun. 2020. Disponível em: <https://www.conjur.com.br/2020-jun-28/constituicao-direito-protecao-dados-tutela-autodeterminacao-informativa>. Acesso em: 10 nov. 2020.

COUTO, R. CASSIO, V. O dever do poder público na proteção de dados pessoais. **Revista Consultor Jurídico**, ago. 2018. Disponível em: <https://www.conjur.com.br/2018-ago-23/opinioao-dever-poder-publico-proteger-dados-pessoais>. Acesso em: 10 nov. 2020.

FRAZÃO, A. **Fundamento da proteção de dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados.** 1. ed. São Paulo: Thomson Reuters Brasil, 2019.

PINHEIRO, P. P. **Proteção de dados pessoais: comentários à Lei 13.709/2018 (LGPD).** 1. ed. São Paulo: Saraiva Educação, 2018.

PONTES, S. **O que fala a Lei Geral de Proteção de Dados Pessoais, Lei 13.709 de 2018.** Disponível em: <https://sergiopontes.jusbrasil.com.br/artigos/614642198/o-que-fala-a-lei-geral-de-protecao-de-dados-pessoais>. Acesso em: 10 nov. 2020.

TEPEDINO, G. FRAZÃO, A. OLIVA, M. D. (org). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro.** 1. ed. São Paulo: Thomson Reuters Brasil, 2019.