UNIVERSIDADE FEDERAL DE SERGIPE
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

KARLA THAÍS NASCIMENTO SANTANA

A INCIDÊNCIA DA LEI GERAL DE PROTEÇÃO DE DADOS NA TUTELA DE DIREITOS FUNDAMENTAIS: O COMBATE AO CAPITALISMO DE VIGILÂNCIA PRATICADO PELAS *BIG TECHS*

São Cristóvão
2024

KARLA THAÍS NASCIMENTO SANTANA

A INCIDÊNCIA DA LEI GERAL DE PROTEÇÃO DE DADOS NA TUTELA DE DIREITOS FUNDAMENTAIS: O COMBATE AO CAPITALISMO DE VIGILÂNCIA PRATICADO PELAS *BIG TECHS*

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade Federal de Sergipe – UFS, como requisito parcial à obtenção do título de Mestre em Direito.

Orientador: Prof. Dr. Lucas Gonçalves da Silva

São Cristóvão

2024

KARLA THAÍS NASCIMENTO SANTANA

A INCIDÊNCIA DA LEI GERAL DE PROTEÇÃO DE DADOS NA TUTELA DE DIREITOS FUNDAMENTAIS: O COMBATE AO CAPITALISMO DE VIGILÂNCIA PRATICADO PELAS *BIG TECHS*

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Direito da Universidade Federal de Sergipe, como parte dos requisitos para a obtenção do Título de Mestre em Direito. Esta dissertação foi julgada e aprovada pela comissão abaixo assinada em ___ de _____ de 2023.

São Cristóvão, Sergipe, Brasil

_____

Prof. Dr. Lucas Gonçalves da Silva – Orientador

Universidade Federal de Sergipe – UFS

_____

Prof. Dr. Henrique Ribeiro Cardoso – Membro Interno

Universidade Federal de Sergipe – UFS

_____

Prof. Dr. Liton Lanes Pilau Sobrinho – Membro Externo

Universidade de Passo Fundo - UPF

Dedico este trabalho aos meus familiares, amigos, aos colegas de curso, aos professores e a todos aqueles que direta ou indiretamente contribuíram para esta conquista.

AGRADECIMENTOS

Em um dos inúmeros momentos difíceis que passei ao longo desses dois anos de jornada acadêmica, entreguei minha vida e meus planos nas mãos de Deus. Foi Ele que me deu forças para enfrentar todas as batalhas advindas até chegar aqui e me abençoa todos os dias com o seu amor infinito. Grata a Ele pela família, e pelas pessoas que colocou em minha vida, que se tornaram essenciais em todos os momentos.

Agradeço, também, por todos os desafios, tropeços e erros, pois, nem tudo é fácil e eles serviram para que eu me tornasse uma pessoa melhor, mais forte e madura.

Aos meus ídolos, meus pais, Edvânia (a mulher guerreira que me inspira em todos os aspectos da vida) e Júnior, e meus avós, Elza (*in memoriam*) e Ananias, e a minha tia-avó Creuza, pelo amor incondicional, por todos os exemplos, ensinamentos e toda a proteção de sempre. Pelo apoio que me foi dado a cada escolha feita. Não mediram esforços para me assistir, e, mesmo com algumas dificuldades, sempre buscaram atender a todos os meus anseios. A caminhada foi árdua, mas, sem dúvidas, tudo se tornou mais fácil com o apoio de vocês. Sem essa base, eu, literalmente, não teria conseguido. À vocês, todo o meu amor e a minha gratidão eterna!

À minha voinha, que, onde quer que esteja, tenho a certeza que está feliz pela concretização desse momento. Não poder comemorar essa conquista com a senhora dói de uma forma inimaginável. Te amo eternamente.

Aos meus tios e primos, e a Marta, por todo o apoio e carinho.

Agradeço ao meu orientador, prof. Dr. Lucas Gonçalves da Silva, pelo incentivo para o ingresso na academia, pela oportunidade que me foi dada, por todo apoio, acolhimento, ensinamentos, compreensão, amizade e força durante esses dois anos.

Aos meus colegas/amigos do mestrado, Hayalla, Rennan, Karen, Camilla, Reginaldo e Yago. Obrigada pelos conselhos, pelas palavras de apoio, pelos puxões de orelha e pelas risadas. Com vocês, a caminhada se tornou mais alegre, fácil e prazerosa.

À Hayalla, meu agradecimento especial. Não tenho palavras para descrever tudo que fez por mim. Sua amizade é um presente de Deus em minha vida. Você é luz e me inspira a ser uma pessoa melhor a cada dia.

À Nara, que me recebeu em Aracaju no momento que eu mais precisei, me ouviu e sempre me incentivou a ser uma pessoa melhor. Você é incrível e eu só tenho a agradecer por tudo que fez/faz por mim.

À Dalva, Rosane, Mateus e Rosendo, que me acolheram e sempre me incentivaram de forma positiva.

Aos meus amigos do Pierre, Luciana, Renata, Mariana e Léo Brucys, que, de alguma forma, sempre estiveram comigo durante a minha vida acadêmica. Saibam que, independente da distância, nossa amizade sempre estará fortalecida e presente na minha vida.

Às minhas amigas de Itabaiana, Isabelle, Tainan, Sunny e Katiane, por toda a força e carinho.

Aos amigos que a Defensoria Pública de Sergipe me presenteou, Fernanda, Nayara e Carla Caroline. Agradeço por todo companheirismo, pela ajuda e confiança.

Aos meus amigos da Faculdade Ages, Murilo e Leandro, que nunca largaram minha mão e sempre estiveram dispostos a me ajudar em qualquer circunstância.

Às minhas amigas Francyele, Mirella, Luiza e Monalisa, pelo carinho de sempre.

À minha amiga e confidente, Valéria, que chegou do nada, no momento em que eu estava descobrindo as dificuldades oriundas da vida adulta e sempre esteve ao meu lado. Agradeço por todo o amor, carinho, paciência e companheirismo. Sei que nossa amizade foi designada por Deus.

Enfim, por último, mas não menos importantes, a todos os demais professores e servidores do Programa de Pós-Graduação em Direito, da Universidade Federal de Sergipe, que dispuseram seu tempo para nos instruir, saibam que cada um marcou de certo modo, a minha jornada. Parabéns a todos pela competência, eficiência, ética e comprometimento com o ensino de qualidade.

RESUMO

A presente dissertação visa demonstrar como a Lei Geral de Proteção de Dados (LGPD) opera na tutela de direitos fundamentais, de modo especial no tocante a privacidade e a proteção de dados. Desde o início do último século, a sociedade vem passando por inúmeras transformações, sobretudo, quando se trata de avanços tecnológicos, em particular as Tecnologias da Informação e Comunicação (TIC). Em virtude disso, fez-se necessário que o direito acompanhasse essas mutações exponenciais na conjuntura social, com fito de proteger direitos fundamentais diretamente por ela afetados, que por sua vez são colocados em risco em prol da dominação e influência de grandes empresas (as *big techs*) que faturam com a manipulação de informações. É perceptível que apesar do avanço da legislação, há muitas dificuldades em efetivar normas que regulem a captação e monetização de dados pelas *big techs*, já que estes se tornaram uma matéria-prima valiosa na sociedade da informação. Ao longo da pesquisa, analisar-se-á o desamparo dos usuários perante a prática de consentir imediatamente com as disposições previstas nos *cookies* e termos de uso de políticas de privacidade desenvolvidos por essas pessoas jurídicas, sem a cautela de averiguar minimamente o que ela dispõe. Além disso, será imperioso discorrer acerca responsabilidade das *big techs* diante do capitalismo de vigilância. Para tanto, utilizou-se a metodologia dedutiva, sendo a abordagem descritiva e exploratória, com uso de fontes primárias e secundárias do direito, como a legislação, doutrina e jurisprudência.

Palavras-chave: Direitos Fundamentais; Capitalismo de Vigilância. Sociedade da Informação. Lei Geral de Proteção de Dados – LGPD. Consentimento.

ABSTRACT

This dissertation aims to demonstrate how the General Data Protection Law (LGPD) operates in the protection of fundamental rights, especially with regard to privacy and data protection. Since the beginning of the last century, society has been going through numerous transformations, especially when it comes to technological advances, in particular Information and Communication Technologies (ICT). As a result, it became necessary for the law to accompany these exponential changes in the social situation, with the aim of protecting fundamental rights directly affected by them, which in turn are put at risk in favor of the domination and influence of large companies (the big ones). techs) that make money from manipulating information. It is noticeable that despite the advancement of legislation, there are many difficulties in implementing standards that regulate the capture and monetization of data by big techs, as these have become a valuable raw material in the information society. Throughout the research, the helplessness of users will be analyzed when faced with the practice of immediately consenting to the provisions set out in cookies and terms of use of privacy policies developed by these legal entities, without taking the precaution of minimally investigating what they have. Furthermore, it will be imperative to discuss the responsibility of big techs in the face of surveillance capitalism. To this end, the deductive methodology was used, with a descriptive and exploratory approach, using primary and secondary sources of law, such as legislation, doctrine and jurisprudence.

Keywords: Fundamental Rights; Surveillance Capitalism. Information Society. General Data Protection Law – LGPD. Consent.

LISTA DE SIGLAS

BDTD - Biblioteca Digital Brasileira de Teses e Dissertações.

CA - *Cambridge Analityca.*

CDH - Conselho de Direitos Humanos das Nações Unidas.

LGPD - Lei Geral de Proteção de Dados.

ONU - Organização das Nações Unidas.

PEC - Proposta de Emenda à Constituição.

RGPD - Regulamento Geral de Proteção de Dados na Europa.

TIC - Tecnologias da Informação e Comunicação.

SUMÁRIO

1 INTRODUÇÃO

O mundo vem passando por inúmeras transformações ao longo dos anos e a principal está diretamente relacionada com o avanço da tecnologia. O século XXI foi marcado pela presença de uma nova realidade, bem distinta da pretérita. As técnicas se desenvolveram em uma velocidade absurda e sucederam a influenciar todas as dimensões da vida social, o que, por sua vez, fez com que juristas passassem a analisar os direitos fundamentais frente às inovações cibernéticas.

Atualmente vive-se uma verdadeira era da informação. A internet, que antes era apenas um vasto campo de oportunidades e possibilidades a serem exploradas, passou a ser considerada como uma “nova sociedade interconectada”, em que são formadas relações com uma velocidade de troca de informação e poder de reprodução muito maior do que jamais seria possível de forma física. Ela deixou de ser um mero instrumento de comunicação entre pessoas, para ter sua própria independência estrutural, que utiliza dados de indivíduos com o objetivo de construir padrões de comportamento e pensamento entre sujeitos.

Essa movimentação e coleta de dados é chamada, de acordo com a professora Shoshana Zuboff (2019), de Capitalismo de Vigilância. Ele utiliza o ser humano e seus comportamentos perante a rede como matéria-prima para a máquina digital, necessariamente revestidos por um manto de anonimato e estreitado por uma falsa ideia de consentimento dos usuários. O que acontece é a “vigilância” dos usuários no ciberespaço pelas plataformas digitais, para definir arquétipos de hábitos e induzir ao consumo de determinadas informações.

A amplificação do uso das ferramentas digitais para o armazenamento de dados facilitou o descobrimento de bases pessoais, tendo como consequência, inúmeros casos de vazamentos de informações não públicas, especialmente quando se trata de grandes empresas que dominam o meio digital, as denominadas *big techs*. Em meio a esse contexto, surgiu a necessidade de criação de meios de proteção de dados, e, consequentemente, da égide da privacidade individual, visto que não é difícil imaginar que o advento da cibercultura causou grande impacto na violação de direitos fundamentais.

A chamada *big data*, utilizada no capitalismo de vigilância, é um exemplo claro de tecnologia que, usada indevidamente, pode fomentar a violação de direitos fundamentais, uma vez que utiliza a análise massiva de dados, muitas vezes sem o

consentimento do usuário, com o objetivo de promover a produção de lucro e controle do mercado das *big techs*. Os algoritmos, por sua vez, também são exemplos de tecnologias que podem causar efeitos negativos nos titulares de dados, devido à utilização da tecnologia para manipular dados, dentro de um limite de tempo, fornecendo de forma confiável um resultado desejado.

Nesses exemplos, “os dados são coletados em prol da própria rede em si, como o *Google* sabendo seus hábitos de pesquisa e moldando os resultados das buscas para algo mais apelativo, como também podem ser vendidos a terceiros, com fins comerciais” (Silva; Siqueira, 2019, p. 204). Há uma vigilância do comportamento das pessoas realizada diariamente com o único e exclusivo objetivo de obtenção de lucro, muitas vezes legitimada no consentimento do titular.

Em razão do avanço da influência da tecnologia na vida contemporânea, em 23 de abril de 2014, foi publicada a Lei nº 12.965/2014, conhecida como “Marco Civil da Internet”. Ela estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Já no mês de agosto de 2020 entrou em vigor a Lei Geral de Proteção de Dados Pessoais (LGPD) (Lei nº 13.709/18), com o objetivo de proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural. Também se cita a Emenda Constitucional nº 115 de 10 de fevereiro de 2022, que incluiu a proteção de dados pessoais entre os direitos e garantias fundamentais e fixou a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

Diante do exposto, surge o questionamento que norteou a pesquisa: a Lei Geral de Proteção de Dados é eficaz para que as *big techs* realizem a coleta, armazenamento, tratamento e utilização dos dados sem ferir os direitos fundamentais a partir das diretrizes nela estabelecidas?

A hipótese se apresenta da seguinte forma: apesar de no Brasil haver uma lei específica, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), a violação de direitos fundamentais é uma realidade vivenciada nos dias atuais, e com ela surgem diversos imbróglios. O maior deles, sem dúvida, é a possibilidade de comprometimento da à privacidade e proteção de dados, tendo em vista o atual mercado digital e seu propósito central, qual seja, a obtenção de lucro através do “novo petróleo”, especialmente porque os indivíduos são seduzidos pelo contorno da facilidade e da individualidade dos produtos e serviços disponibilizados e, em razão

disso, consentem em ter seus dados utilizados sem suscitar as consequências futuras dessa simples ação do cotidiano.

Neste contexto, o objetivo geral deste estudo foi dissertar, com base na doutrina, legislação e jurisprudência, acerca da coleta e tratamento de dados dos usuários pelas *big techs*, tendo como fundamento a eficácia da proteção de direitos fundamentais perante a LGPD. Discorrer de forma profunda sobre essa temática será essencial para trazer à sociedade reflexões acerca das consequências do capitalismo de vigilância, uma vez que, ao longo deste trabalho analisar-se-á o desamparo dos usuários perante a prática de aceitar imediatamente *cookies* e termos de uso da política de privacidade desenvolvida pelas empresas, sem a cautela de analisar minimamente o que ela dispõe.

Para desenvolvê-lo, os seguintes objetivos específicos foram delimitados: 1) compreender o comportamento da LGPD frente a Nova Ordem Econômica, com o chamado capitalismo de vigilância; 2) expor a importância dos dados na sociedade da informação; 3) discorrer sobre a estrutura da LGPD, seus principais conceitos, nomenclaturas, princípios fundamentadores, aspectos positivos, negativos; 4) entender como se deu a necessidade de criação do Regulamento Geral de Proteção de Dados na Europa – RGPD e sua repercussão no ordenamento jurídico pátrio; 5) analisar os limites da adequação da LGPD no setor empresarial, especialmente quando se trata da ideia de consentimento, a partir da compreensão dos seus tópicos deficitários com a análise da jurisprudência e busca por uma “solução” para o capitalismo ilícito de dados.

O interesse a respeito do tema surgiu em virtude das inúmeras discussões traçadas no Grupo de Pesquisa em Direito Digital coordenado pelo Professor Dr. Lucas Gonçalves da Silva, em especial, os debates desenvolvidos após a leitura da obra Capitalismo de Vigilância, da autora Shoshana Zuboff. O que se percebeu nessas reflexões é que, em que pese a grande evolução das tecnologias da informação, não houve avanço no âmbito jurídico que pudesse possibilitar a aplicação adequada da legislação perante casos envolvendo violações de direitos fundamentais, bem como a responsabilidade das *big techs* diante desse cenário.

Para produção da corrente dissertação, foi utilizada a metodologia dedutiva, sendo a abordagem quantitativa, descritiva e exploratória, quanto ao tipo de pesquisa bibliográfica, foi desenvolvido tanto através de pesquisa teórica, como técnica, no decurso do estudo das fontes primárias e secundárias do Direito, dentre elas a

legislação internacional, nacional, doutrinas nas áreas de Direitos Humanos e Constitucional e jurisprudências.

No que se refere à literatura pertinente ao tema de pesquisa, foram utilizados artigos, teses, dissertações e documentos, levantados através das bases de dados disponibilizadas através do Portal Periódicos Capes, Plataforma SciElo, Biblioteca Digital Brasileira de Teses e Dissertações (BDTD), Google Scholar, JusBrasil, entre outros. Para atingir os objetivos gerais e específicos anteriormente expostos, foi necessário dividir o trabalho em três capítulos, os quais apresentaremos a seguir.

O primeiro capítulo abordou acerca das noções de direitos fundamentais, tendo em vista que a temática central do estudo gira em torno da necessidade de proteção destes frente à ascensão das novas tecnologias. Também foi imprescindível traçar o histórico da evolução do direito à proteção de dados e privacidade no Brasil (trazendo uma introdução à proteção de dados no direito europeu), com o intuito de entender como se deu a necessidade de positivação destes diante das novas conjunturas sociais. Por fim, apresentou-se um conceito básico para a compreensão acerca do tema, qual seja, a sociedade da informação.

O segundo capítulo versou sobre o capitalismo de vigilância sob uma ótica negativa da monetização de dados, no intuito de encontrar o momento em que a competitividade das grandes empresas (as *big techs*) provocou uma mudança no comportamento das máquinas, de modo que elas desenvolveram meios de conhecer os comportamentos humanos e a partir disso molda-los para um fim específico. Em seguida, descreveu-se acerca do protagonismo das *big techs* na sociedade da informação. Por fim, dissertou-se sobre a norma europeia que inspirou a criação da Lei Geral de Proteção de Dados no Brasil, qual seja, o Regulamento Geral de Proteção de Dados (RGPD).

No último capítulo foi descrito acerca do objeto principal de estudo da presente pesquisa: a Lei nº 13.709/2018 - Lei Geral de Proteção de Dados – LGPD, elencando elementos da sua estrutura, principais conceitos, nomenclaturas, princípios fundamentadores, atua na proteção do direito à privacidade e a proteção de dados. Além disso, durante os estudos foi possível identificar alguns tópicos deficitários da Lei Geral de Proteção de Dados – LGPD, em especial a ideia de consentimento do usuário quando utilizada como única forma de legitimar a captação e tratamento de dados, além de trazer uma reflexão acerca de como a jurisprudência tem se comportado diante dos inúmeros casos de violação dos direitos fundamentais em

epígrafe. Para tanto, foi preciso levantar o debate sobre o modo como a vigilância operada pelas empresas pode levar à violação da privacidade e proteção de dados, bem como as soluções jurídicas para que haja um equilíbrio entre a proteção dos dados pessoais e a comercialização de dados de forma lícita.

2 OS DIREITOS FUNDAMENTAIS NA SOCIEDADE DA INFORMAÇÃO

O presente capítulo aborda as noções de direitos fundamentais, tendo em vista que a temática central do estudo gira em torno da necessidade de proteção destes frente à ascensão das novas tecnologias. Também foi imprescindível traçar o histórico da evolução do direito à proteção de dados e privacidade no Brasil, com o intuito de entender como se deu a necessidade de positivação destes diante das novas conjunturas sociais. Por fim, apresentou-se um conceito básico para a compreensão acerca do tema, qual seja, a sociedade da informação.

2.1 AS PRINCIPAIS NOÇÕES SOBRE DIREITOS FUNDAMENTAIS

A Constituição brasileira, promulgada em 5 de outubro de 1988, foi considerada como o marco da redemocratização do país, uma vez que surgiu após o período da Ditadura Militar. Como uma das formas de reestruturar o Estado moderno, o legislador positivou uma gama de direitos fundamentais, logo, pode-se dizer que a história dos direitos fundamentais coincide com o constitucionalismo. Pardo (1998, p. 05) explica que o constitucionalismo moderno passa por variações históricas de acordo com a evolução dos direitos que garante, reforçando a tese de origem congênita do constitucionalismo e a doutrina dos direitos fundamentais.

Essa nova categoria é capaz de assegurar, no campo do próprio direito privado, a proteção daqueles direitos imprescindíveis ao ser humano, direitos que não se limitavam a uma liberdade ilusória e vazia, direitos superiores à própria liberdade, direitos a salvo da vontade do seu titular, direitos indisponíveis, direitos inalienáveis, direitos inatos (SCHEREIBER, 2014, p. 4).

Os direitos fundamentais traçaram um caminho até chegar à atual concepção, sendo sua consolidação marcada por uma maturação histórica. Inicialmente, tem-se o pensamento cristão como impulsionador da ideia de dignidade humana. Logo após, o direito natural, isto é, aqueles que são inerentes ao ser humano desde sua criação, ganham pertinência congênita. O direito natural foi relatado de forma assídua por meio de teorias contratualistas de Thomas Hobbes (1588 - 1679), John Locke (1632 - 1704), Rousseau e Montesquieu, que trouxeram à tona a necessidade do Estado ser garantidor de direitos e servir aos cidadãos através de um pacto social.

O homem, antes de ter direitos civis, é produto da história, tem direitos naturais que os precedem; e esses direitos naturais são o fundamento de todos os direitos civis. No entanto, estes, por si só, não eram suficientes para que fosse assegurada a dignidade da pessoa humana em sua plenitude. Notou-se, então, a necessidade de positivação (BOBBIO, 2004, p. 82).

Destaca-se que a relação entre Estado e indivíduo deve ser encarada de forma equilibrada. Nesse sentido, Bobbio (1992, p. 04) ensina que

> [...] a afirmação dos direitos do homem deriva de uma radical inversão de perspectiva, característica da formação do Estado moderno, na representação da relação política, ou seja, na relação Estado/cidadão ou soberano/súditos: relação que é encarada, cada vez mais, do ponto de vista dos direitos dos cidadãos não mais súditos, e não do ponto de vista dos direitos do soberano, em correspondência com a visão individualista da sociedade (...) no início da idade moderna.

De certo, tratar sobre toda a história dos direitos fundamentais com riqueza de detalhes, desde a concepção do jusnaturalismo até os dias atuais, nos faria incorrer em uma análise prolixa ao longo do estudo. Logo, passa-se à conceituação que, por sua vez, também se torna hermética, em virtude da ampliação e transformação desses direitos ao longo do processo histórico.

Entende-se que são utilizadas inúmeras terminologias para designar o que entendemos enquanto direitos fundamentais. Não obstante, de acordo com José Afonso da Silva (2016, p. 180) direitos fundamentais do homem constitui a expressão mais adequada a este estudo, porque, além de referir-se a princípios que resumem a concepção do mundo e informam a ideologia política de cada ordenamento jurídico, é reservada para designar, no nível do direito positivo, aquelas prerrogativas e instituições que ele concretiza em garantias de uma convivência digna, livre e igual de todas as pessoas.

O adjetivo “fundamentais” é utilizado para tratar de situações jurídicas sem as quais a pessoa humana não se realiza, não convive e, às vezes nem mesmo sobrevive; fundamentais do homem no sentido de que a todos, por igual, devem ser, não apenas formalmente reconhecidos, mas concreta e materialmente efetivados (SILVA, 2016, p. 180). Em síntese, é o

> [...] conjunto de facultades e ínstitucíones que, en cada momento histórico, concretan las exigencias de la dignidad, la libertad y la igualdad humanas, las

> cuales deben ser reconocidas positivamente por los ordenamientos jurídicos a nível nacional e internacional (PEREZ, 2004, p. 43).

Silva (2016, p. 183) elenca as características dos direitos fundamentais. Para ele, a concepção naturalista propõe a tese de que são inatos, absolutos, invioláveis (intransferíveis), imprescritíveis e irrenunciáveis. Essas peculiaridades inerentes aos direitos fundamentais refletem a magnitude da sua importância para um ordenamento jurídico. Frise-se que, atualmente, a doutrina entende que não há direito fundamental absoluto. Em verdade, existe a divisão entre absolutos e relativos. Os primeiros são

> [...] os que existem não conforme os cria ou regula a lei, mas a despeito das leis que os pretendam modificar ou conceituar (assim: a liberdade pessoal, a inviolabilidade do domicílio ou da correspondência), enquanto os relativos existem, mas valem conforme a lei (assim: os direitos de contrato, de comércio e indústria e o direito de propriedade). (SILVA, 2016, p. 183).

Os direitos fundamentais também sofrem alterações em suas especificidades a depender do momento histórico, “ou seja, nascidos de modo gradual, não são todos de uma vez e nem de uma vez por todas” (BOBBIO, 2004, p. 25). Com o objetivo de ilustrar tal processo, passou a ser difundida – por meio da voz de Karel Vasak, a partir de conferência proferida em 1979 no Instituto Internacional de Direitos Humanos, em Estrasburgo – a ideia de que a evolução dos direitos (humanos e fundamentais) poderia ser compreendida mediante a identificação de três “gerações” de direitos, havendo quem defenda a existência de uma quarta e até mesmo de uma quinta e sexta geração de direitos humanos e fundamentais (MARINONI; MITIDIERO; SARLET, 2017, p. 339). Por essa razão, a doutrina em dimensões, terminologia que valoriza a óptica histórica e evolutiva de novos direitos.

Essa distinção entre gerações dos direitos fundamentais é estabelecida apenas com o propósito de situar os diferentes momentos em que esses grupos de direitos surgem como reivindicações acolhidas pela ordem jurídica. Deve-se ter presente, entretanto, que falar em sucessão de gerações não significa dizer que os direitos previstos num momento tenham sido suplantados por aqueles surgidos em instante seguinte (MARINONI; MITIDIERO; SARLET, 2017, p. 343).

Os direitos fundamentais de primeira dimensão estão associados com a liberdade derivada do contexto da Revolução Francesa, e inseridos nas primeiras constituições escritas. São direitos em que não desponta a preocupação com

desigualdades sociais. O paradigma de titular é o homem individualmente considerado (MENDES; BRANCO, 2012, p. 178).

Nesse contexto, assumem particular relevo os direitos à vida, à liberdade, à propriedade e à igualdade perante a lei, posteriormente complementados por um leque de liberdades, incluindo as assim denominadas liberdades de expressão coletiva (liberdades de expressão, imprensa, manifestação, reunião, associação etc.), e pelos direitos de participação política, tais como o direito de voto e a capacidade eleitoral passiva, revelando, de tal sorte, a íntima correlação entre os direitos fundamentais e a democracia (MARINONI; MITIDIERO; SARLET, 2017, p. 341). Cita-se alguns documentos pioneiros em sua positivação, como a Carta Magna de 1215 do Rei "João Sem Terra"; A Paz de Wetstfália; O Hábeas Corpus e as Declarações de Direitos de 1776 (EUA), além da Francesa de 1789.

Paulo Bonavides (2006, p. 569) descreve que os direitos fundamentais de primeira dimensão representam exatamente os direitos civis e políticos, que correspondem à fase inicial do constitucionalismo ocidental, mas que continuam a integrar os catálogos das Constituições atuais (apesar de contar com alguma variação de conteúdo), o que demonstra a cumulatividade das dimensões.

Já os de segunda dimensão estão relacionados à igualdade, bem como dos direitos surgidos com o advento do Estado social, com o advento da Revolução Industrial no século XIX e o contexto pós Primeira Guerra Mundial e, marcado pelo grande desenvolvimento tecnológico que alterou de forma significativa a forma com que as mercadorias da época eram produzidas. Como o trabalhador era visto como sujeito sem direitos, surgem as primeiras reinvindicações com viés social, pautadas, mais uma vez, na dignidade da pessoa humana.

> Tais direitos fundamentais, que embrionária e isoladamente já haviam sido contemplados nas Constituições francesas de 1793 e 1848, na Constituição brasileira de 1824 e na Constituição alemã de 1849 (que não chegou a entrar efetivamente em vigor), caracterizam-se, ainda hoje, por assegurarem ao indivíduo direitos a prestações sociais por parte do Estado, tais como prestações de assistência social, saúde, educação, trabalho etc., revelando uma transição das liberdades formais abstratas para as liberdades materiais concretas, utilizando-se a formulação preferida na doutrina francesa. (IBIDEM, 2017, p. 342).

O princípio da igualdade ganha relevância nessa segunda geração dos direitos fundamentais, a ser atendido por direitos a prestação e pelo reconhecimento de liberdades sociais – como a de sindicalização e o direito de greve. Os direitos de

segunda geração são chamados de direitos sociais, não porque sejam direitos de coletividades, mas por se ligarem a reivindicações de justiça social – na maior parte dos casos, esses direitos têm por titulares indivíduos singularizados (MENDES; BRANCO, 2020, p. 179). Logo, eles posem ser considerados uma densificação do princípio da justiça social, além de corresponderem a reivindicações das classes menos favorecidas, de modo especial da classe operária, a título de compensação, em virtude da extrema desigualdade que caracterizava (e, de certa forma, ainda caracteriza) as relações com a classe empregadora, notadamente detentora de um maior ou menor grau de poder econômico (SARLET, 2007, p. 50).

Traçando um quadro comparativo, pode-se afirmar que

> Os direitos de primeira geração tinham como finalidade, sobretudo, possibilitar a limitação do poder estatal e permitir a participação do povo nos negócios públicos. Já os direitos de segunda geração possuem um objetivo diferente. Eles impõem diretrizes, deveres e tarefas a serem realizadas pelo Estado, no intuito de possibilitar aos seres humanos melhores qualidade de vida e um nível de dignidade como pressuposto do próprio exercício da liberdade. Nessa acepção, os direitos fundamentais de segunda geração funcionam como uma alavanca ou uma catapulta capaz de proporcionar o desenvolvimento do ser humano, fornecendo-lhe as condições básicas para gozar, de forma efetiva, a tão necessária liberdade (MARMELSTEIN, 2008, p. 50).

Por sua vez, a terceira dimensão é a de direitos difusos, como fraternidade e solidariedade. Eles trazem como nota distintiva o fato de se desprenderem, em princípio, da figura do homem-indivíduo como seu titular, destinando-se à proteção de grupos humanos (povo, nação), caracterizando-se, consequentemente, como direitos de titularidade transindividual (coletiva ou difusa) (MARINONI; MITIDIERO; SARLET, 2017, p. 343). Dentre os direitos fundamentais da terceira dimensão mais citados, cumpre referir os direitos à paz, à autodeterminação dos povos, ao desenvolvimento, ao meio ambiente e qualidade de vida, bem como o direito à conservação e utilização do patrimônio histórico e cultural e o direito de comunicação (IBIDEM, 2017, p. 343). São direitos reivindicados em razão do processo de globalização.

Na terceira dimensão,

> Um novo polo jurídico de alforria do homem se acrescenta historicamente aos da liberdade e da igualdade. Dotados de altíssimo teor de humanismo e universalidade, os direitos da terceira geração tendem a cristalizar-se no fim do século XX enquanto direitos que não se destinam especificamente à proteção dos interesses de um indivíduo, de um grupo ou de um determinado Estado. Tem primeiro por destinatário o gênero humano mesmo, num

> momento expressivo de sua afirmação como valor supremo em termos de existencialidade concreta (BONAVIDES, 2006, p. 569).

Há controvérsias doutrinárias acerca da existência ou não de direitos de quarta, quinta e até mesmo sexta dimensão. Os que defendem a existência de uma quarta dimensão atrelam à proteção dos direitos advindos do desenvolvimento tecnológico. Bobbio (2004, p. 25) ensina que a quarta dimensão tem a ver com "os efeitos cada vez mais traumáticos da pesquisa biológica". Já Uadi Bulos (2007, p. 404) assegura que os direitos de quarta geração estão conexos "à informática, softwares, biociências, eutanásia, alimentos transgênicos, sucessão dos filhos gerados por inseminação artificial, clonagens, dentre outros conhecimentos ligados à engenharia genética".

Além dos direitos trazidos a título exemplificativo por Bobbio (2004) e Uadi Bulos (2007), é importante pontuar que os direitos de quarta dimensão estão correlacionados às questões emergentes da era da globalização. Esses direitos foram introduzidos no âmbito jurídico pela globalização política, compreendem o direito à democracia, informação e pluralismo. Os direitos fundamentais de quarta dimensão compendiam o futuro da cidadania e correspondem à derradeira fase da institucionalização do Estado social sendo imprescindíveis para a realização e legitimidade da globalização política (MARCELO NOVELINO, 2017, p. 229).

Através da análise doutrinária acima, é possível inferir que os direitos fundamentais trazidos à baila nesse estudo, tal qual, a privacidade e proteção de dados, podem ser diretamente atrelados à quarta dimensão. Isto porque, atualmente, a privacidade ganhou novos contornos com o avanço tecnológico. Como estar-se-á diante de parte do estudo central da presente dissertação, o próximo tópico tratará de forma mais aprofundada acerca da temática.

2.2 EVOLUÇÃO DO DIREITO À PRIVACIDADE E À PROTEÇÃO DE DADOS

No estudo do direito à privacidade, é essencial compreender os contornos que envolvem a terminologia "vida privada", bem como quais as consequências jurídicas do seu significado. Há uma problemática envolvendo esse termo: a ausência de definição exata do seu sentido. Morais (2020, p. 202) explica que a falta de uma definição unitária que reflita o conteúdo semântico do direito à privacidade é percebida inclusive nos enunciados normativos que visam sua tutela. No âmbito dos direitos

humanos são utilizadas as expressões: vida privada, vida familiar, inviolabilidade do domicílio e da correspondência.

Gilberto Haddad Jabur (2000, p. 260) ensina que o direito à privacidade decorre do direito à liberdade, na medida em que o primeiro abriga o direito à quietude, à paz interior, à solidão e ao isolamento contra a curiosidade pública, em relação a tudo o quanto possa interessar à pessoa, impedindo que se desnude sua vida particular; enquanto o segundo resguarda o direito a uma livre escolha daquilo que o indivíduo pretende ou não expor para terceiros, protegendo o seu círculo restrito da forma como lhe aprouver.

Celso Bastos (1989, p. 260) explica que a privacidade é a

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

Costa Júnior (2004) cita que na expressão “direito à intimidade” são tutelados dois interesses, que se somam: o interesse de que a intimidade não venha a sofrer agressões; e o de que não venha a ser divulgada. O direito, porém, é o mesmo. O que pode assumir uma gama diversa são os interesses protegidos pelo direito. São duas esferas de interesses, abarcadas no raio de proteção do mesmo direito. No âmbito do direito à intimidade, portanto, podem ser vislumbrados esses dois aspectos: a invasão e a divulgação não autorizadas da intimidade legitimamente conquistada. Em termos de conteúdo, todavia, não deve prevalecer a distinção.

As palavras “vida privada, intimidade, privacidade e domicílio” podem ser consideradas como sinônimos. No entanto, uma parte da doutrina, à exemplo de Tércio Sampaio (1993), entende que não há equivalência, mas sim uma diferenciação de sentidos, que irá interferir na aplicabilidade da norma.

A vida privada foi utilizada na Teoria dos Círculos Concêntricos, baseada nas pesquisas de Heinrich Hubmann e Heinrich Henkel (1967) na Alemanha. Para Hubmann (1953, p. 30-40) a tutela da privacidade é dividida em três eixos: *privatsphare* (direito à privacidade em sentido estrito), o *vertrauenssphare*, (direito à intimidade) e o *geheimphare ou vertraulichkeitssphare* (direito ao segredo). Seriam o primeiro, segundo e terceiro (núcleo) dos círculos, respectivamente.

Hubmann (1953) classificou o direito geral da personalidade em três círculos concêntricos (esfera secreta, íntima e privada), dentro dos quais se desdobraria a personalidade humana. Para o autor, tem-se como primeira e mais densa entre elas, a esfera do segredo (Geheims¬phäre) que garante a proteção absoluta dos indivíduos na sua própria pessoa, como por exemplo, em suas posições filosóficas, políticas, orientação sexual, etc. Esta esfera constitui-se no âmbito cujo o indivíduo exerce total controle e poderá manter em total segredo fatos e informações da coletividade (HUBMANN, 1953, p. 30-40).

A intimidade é definida pelo autor como a esfera intermediária (Vertrauens¬phäre), que engloba informações mais restritas sobre o ser humano, compartilhadas com reduzido número de pessoas que possuem relações familiares, afetivas e profissionais com o indivíduo ou com pessoas que têm acesso a informações de forma privilegiada em razão do status profissional (i.e, psicólogos, padres e advogados, profissionais de saúde, etc.). É neste círculo que se encontram protegidos o sigilo domiciliar, profissional e das comunicações telefônicas, que sofrem restrições mais agudas para sua abertura.

Por último, o autor caracteriza a privacidade como parte da esfera da vida privada em sentido estrito (Privatsphäre), em que repousam as relações interpessoais menos densas, na qual não há um amplo grau de conhecimento da vida alheia. O acesso ao público, na esfera da vida privada, é apontado pelo autor como restrito, mas seu grau de adstrição é o menor dentre as três esferas, sendo o interesse público uma justificativa adequada, em alguns casos, para acesso e revelação de informações privadas (HUBMANN, 1953, p. 30-40).

Frota (2007, p. 459) ensina que a extremidade da vida particular mais perceptível ao observador externo e menos reveladora da personalidade de cada um, serve de palco à faceta material da esfera privada e às relações interpessoais perfunctórias, ilustradas pelas amizades circunscritas ao coleguismo. Nessa seara perfilam quer noções ligeiras sobre a rotina diária do indivíduo, quer os dados indicativos do seu patrimônio.

Segundo ele, no bojo da esfera privada está contida a esfera da intimidade (*Vertrauensphäre*), ou esfera confidencial (*Vertraulichkeitssphäre*). Dela participam somente aquelas pessoas nas quais o indivíduo deposita certa confiança, com as quais mantém certa intimidade. Fazem parte desse campo conversações ou acontecimentos íntimos, dele estando excluídos não apenas o público em geral, como

é óbvio; bem assim, determinadas pessoas, que privam com o indivíduo num âmbito mais amplo. Por fim, o direito ao segredo (IBIDEM, 2007, p. 459).

Já a palavra privacidade, de acordo com Morais (2018, p. 203), enquanto direito subjetivo, tem origem em 1890, quando juristas norte-americanos Warren e Brandeis revisitaram o conceito jurídico de propriedade material para configurar evolutivamente o direito imaterial à privacidade. Os autores, através da linha interpretativa analógica e por meio de precedentes judiciais da Suprema Corte dos EUA, concluíram que havia um estatuto jurídico constitucional capaz de garantir o direito geral à privacidade como *right to be left alone*, conceituando-o como aquele que protege o direito de estar só do indivíduo, independentemente da forma de expressão.

As teorias supramencionadas interferiram na definição de privacidade em ordenamentos jurídicos de diversos países, no entanto, de forma aprimorada, tendo em vista que o direito à privacidade passou a ter importância mais acentuada na medida em que a economia migrou para o meio digital. O desenvolvimento da tecnologia e do consumo de produtos e serviços no ciberespaço refletiu mudanças na captação e armazenamento de dados. Isso ecoa de forma direta no direito à privacidade e evidencia a possibilidade de violação dessa garantia constitucional, ao passo em que para ter acesso à internet e a tudo que ela disponibiliza, é necessário deixar um rastro de informações.

Em particular, na visão contemporânea o direito à privacidade decorre exclusivamente do livre desenvolvimento da personalidade da pessoa humana, visto que o simples fato de viver em sociedade já afasta, por si só, o anonimato. (CACHAPUZ, 2006, p. 53). Marcelo Pereira (2004, p. 140) assegura que o direito à intimidade seria (...) o poder das pessoas de controlar suas informações pessoais, as quais, ainda que não formem parte da vida privada das mesmas, possam revelar aspectos de sua personalidade.

Em 1846, foi publicada na Alemanha, a obra de David Augusto Röder, com o título "*Grundzüge des Naturrechts oder der Rechtsphilosophie"*, em que o autor descreveu alguns atos violadores do direito à privacidade. No ano de 1858, o Tribunal de Séné reconheceu pela primeira vez na sua jurisprudência, a garantia em epígrafe, ao reconhecer à família de uma famosa atriz o direito de não publicarem fotografias da sua morte (SAMPAIO, 1998, p. 55-60).

Em 1890 publicaram um artigo nos Estados Unidos com o título *Right to privacy*, que tinha como escopo a análise de precedentes da Suprema Corte acerca de temas como propriedade, direitos autorais e difamação. Eles descreveram não só a proteção da honra, mas também a divulgação de quaisquer informações sem a autorização do titular.

Através de uma análise pormenorizada da doutrina, depreende-se que o direito à privacidade já era assegurado no século XVI na Inglaterra, com o chamado princípio da inviolabilidade de domicílio. No entanto, apenas no século XIX a privacidade ganhou novos contornos.

Na América e na Europa, até a primeira metade do século XIX a defesa do direito à privacidade confundiu-se com a da propriedade privada e da honra. Mas a partir da segunda metade do século XIX, a tutela da privacidade recebeu novos contornos. No século XX, as inovações tecnológicas provocaram súbitas mudanças no conceito de privacidade, elevando o risco de violação. (NAVARRO, 2014, p. 02).

A Declaração Universal dos Direitos do Homem, de 10 de dezembro de 1948, reconheceu o direito à privacidade em âmbito internacional em seu art. 12[1]. Já em 1969 o art. 11 da Convenção Americana sobre Direito Humanos, no Pacto de São José da Costa Rica reproduziu a redação da Declaração Universal dos Direitos do Homem.

Já em 1967, o tema foi objeto de discussão em uma comissão internacional de juristas na Conferência Nórdica sobre o Direito à Intimidade, realizada em Estocolmo. Em 1969 o art. 11 da Convenção Americana sobre Direito Humanos, no Pacto de São José da Costa Rica reproduziu a redação da Declaração Universal dos Direitos do Homem[2].

No direito internacional, é possível citar o sistema global de direitos humanos e os sistemas regionais. Norberto Bobbio (1988, p. 201) sustenta que os direitos humanos nascem como direitos naturais universais, desenvolvem-se como direitos

[1] "Art. 12 Ninguém será objeto de ingerências arbitrárias em sua vida privada, sua família, seu domicílio ou sua correspondência, nem de ataques a sua honra ou a sua reputação. Toda pessoa tem direito à proteção da lei contra tais ingerências e ataques".

[2] "Artigo 11. Proteção da honra e da dignidade 1. Toda pessoa tem direito ao respeito de sua honra e ao reconhecimento de sua dignidade. 2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação. 3. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas".

positivos particulares (quando cada Constituição incorpora Declarações de Direito), para finalmente encontrarem sua plena realização como direitos positivos universais.

Como se verifica, a internacionalização dos direitos tem início no período pós-Segunda Guerra Mundial, como forma de prevenir/reprimir as atrocidades cometidas pelo movimento nazista na Alemanha contra os judeus. Com esse objetivo, é criada em 1945 a Organização das Nações Unidas (ONU), para a proteção dos direitos humanos. Logo após, em 1948, a Declaração Universal dos Direitos Humanos é adotada como norma internacional de cunho global para proteção de direitos humanos.

O sistema global incorpora normas de alcance universal. Já os sistemas regionais de direitos humanos são integrados pelos sistemas interamericano, europeu e africano. A sua incorporação à Organização das Nações Unidas (ONU) surgiu com o objetivo de compatibilizar compromissos globais com locais, conforme alcance geográfico de cada continente, ganhando dimensão o chamado glocal. Essa expressão é utilizada por Paul Soriano, por meio da leitura de Manuel Castells de que local significa os “nós” – nós de valor acrescentado aos fluxos econômicos e lugares de vida social Assim, no "glocal, " o "local" representaria os "nós" da rede global e integraria as resistências, bem como as contribuições das formações identitárias locais e regionais na construção dos direitos humanos (HABIBUL, 2004, p. 78).

No sistema europeu de direitos, em algumas situações, a Corte Europeia de Direitos Humanos julga casos acerca de possíveis violações da privacidade. Com o objetivo de demonstrar isso, Leonardo Stoll de Morais (2018, p. 206) realizou uma revisão jurisprudencial do direito à privacidade no sistema regional europeu de direitos humanos.

A pesquisa foi realizada em 83 casos julgados pela Corte. De acordo com ele, ela aplica o termo vida privada para proteger as situações jurídicas subjetivas relacionadas à identidade pessoal, à integridade, à imagem, aos dados pessoais e sensíveis do indivíduo (IBIDEM, 2018, p. 206).

Já o termo vida familiar abrange às situações jurídicas subjetivas associadas às relações formais e informais, às decisões reprodutivas e o controle do poder familiar. Para a Corte, o termo domicílio não se refere a um lugar em que a pessoa natural tem ânimo de permanecer, ao revés abrange lugares como em albergues, o estabelecimento comercial ou a casa do indivíduo. Em relação ao termo correspondência, a Corte protege as situações jurídicas subjetivas envolvendo

manifestações escritas e orais, externadas por meio de cartas, e-mails, rede sociais e via telefone (MORAIS, 2018, p. 206).

Os resultados indicam que o tratamento conferido à privacidade pelo sistema regional europeu de direito humanos consolida o direito à autonomia dos indivíduos, marcando assim, o desenvolvimento da personalidade dos seres humanos, do ponto de vista individual e relacional (MORAIS, 2018, p. 205). Eles utilizam como parâmetro o art. 8º da Convenção para a Proteção dos Direitos Humanos. No entanto, a aplicação do conceito privacidade é definido de acordo com a análise de cada caso concreto.

Apesar de não haver na pesquisa supracitada menção às jurisprudências da Corte Europeia de Direitos Humanos quanto à utilização da Diretiva 2006/24/CE do Parlamento Europeu, que constitui uma norma essencial na proteção de dados no sistema regional europeu de direitos.

A Diretiva 2006/24/CE é uma norma relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva 2002/58/CE. Ela constitui um grande avanço para o ordenamento jurídico europeu e exige que os Estados-Membros protejam os direitos e as liberdades das pessoas singulares no que diz respeito ao tratamento de dados pessoais, nomeadamente o seu direito à privacidade, com o objetivo de assegurar a livre circulação de dados pessoais na comunidade.

Outro exemplo histórico dessa agenda de integração entre o vetor de integração econômica fomentada pela tecnologia e a tutela de direitos foi justamente a aprovação, em 1980, das Diretrizes Gerais da OCDE (Organização para a Cooperação e Desenvolvimento Econômico) sobre Privacidade e o Fluxo Transfronteiriço de Dados Pessoais, revisadas em 2013 (MENDES E FONSECA, 2020, p. 512).

Além disso, cita-se o Regulamento Geral de Proteção de Dados (RGPD) aprovado em 2016, em substituição a Diretiva de Proteção de Dados de 1995. O RGPD tem como objetivo principal harmonizar as leis de privacidade de dados no bloco europeu, regulando o processamento por indivíduos, empresas ou organizações de dados pessoais relacionados a indivíduos do bloco.

Nesse sentido, as grandes novidades trazidas pelo RGPD foram: o fortalecimento dos direitos dos indivíduos sobre seus dados; a obrigação de

harmonização das normas sobre o tema para os reguladores europeus; e maior responsabilidade pra as empresas em relação aos dados pessoais que coletam, com sanções mais duras para aquelas que não agirem em conformidade com as novas regras (CONSUMERS INTERNATIONAL, 2018, p. 1). A União Europeia também dispõe de um grupo para auxiliar a implementação do Regulamento Geral, o *Multistakeholder Expert Group*.

Na Europa, o art. 8º da Convenção para a Proteção dos Direitos Humanos e das Liberdades Fundamentais prevê a proteção à vida privada e familiar, do domicílio e da correspondência[3].

Na 34ª sessão do Conselho de Direitos Humanos das Nações Unidas (CDH), a 3ª Comissão da Assembleia Geral das Nações Unidas (ONU) aprovou a resolução intitulada “Direito à privacidade na era digital”, apresentada pelo Brasil, Alemanha, Áustria, Liechtenstein, México e Suíça. Uma das premissas é reafirmar os direitos previstos no Pacto Internacional sobre Direitos Civis e Políticos, em particular, o direito à privacidade e a não ser submetido a ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, bem como o direito à proteção da lei contra essas ingerências ou ofensas, de acordo com o art. 12 da Declaração Universal dos Direitos Humanos e o art. 17 do Pacto Internacional sobre Direitos Civis e Políticos

O que se observa é que no passado a privacidade, entendida nos termos que aqui delineamos, não possuía a mesma importância como direito fundamental e humano, diferente do contexto atual. Segundo David H. Flaherty (1990-1991, pp. 831-855) historicamente, a privacidade consistia em um conceito não previsto em lei, no sentido de que os indivíduos reivindicavam sua privacidade individualmente, de forma mais ampla ou mais restrita, defendendo-se livremente quando havia qualquer ameaça.

Essa concepção foi drasticamente alterada desde o início da industrialização no século XIX. Apesar dos esforços para manutenção da privacidade, fez-se

[3] “Direito ao respeito pela vida privada e familiar:1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros”.

necessária a instituição de autoridades e, ainda, a edição de leis para preservação deste direito.

No Brasil, a necessidade de proteção de dados se tornou mais acentuada na medida em que a economia migrou para o meio digital. O desenvolvimento da tecnologia e do consumo de produtos e serviços no ciberespaço refletiu mudanças na captação e armazenamento de dados. Isso ecoou de forma direta no direito à privacidade e apontou a possibilidade de violação dessa garantia constitucional, ao passo que, para ter acesso à internet e a tudo que ela disponibiliza, é necessário deixar um rastro de informações.

Essas, em sua maioria, são armazenadas na *big data* e utilizadas de forma mercantilizada em propagandas de marketing invasivas, além da difusão de conteúdos programados de acordo com as bases coletadas através do consentimento do usuário, em especial ao aceitar termos e uso e política de cookies. No ano de 1988 a Constituição Federal do Brasil positivou o direito à privacidade no art. 5º, incisos X, XI e XII[4].

Em 23 de abril de 2014, foi publicada a Lei nº 12.965/2014[5], conhecida como Marco Civil da Internet. Ela estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Para Paesani (2014, p. 65) o Marco Civil da Internet foi uma conquista para a inclusão digital do país, que contou com a participação social, instituindo regras que contribuíram para a proteção da privacidade na rede mundial de computadores, porém, não a tratou com o merecido cuidado.

Com isso, foi criado o Decreto nº 8771/2016 para regulamentar o Marco Civil da Internet. Entretanto, tais legislações não trataram de forma efetiva a questão da proteção de dados pessoais e muito menos tutelaram seu tratamento, fazendo com

[4] "Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial; (Vide Lei nº 13.105, de 2015) (Vigência); XII - e 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; (Vide Lei nº 9.296, de 1996)".

[5] Lei 12.965/2014: Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei; Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação. (BRASIL, 2014)

que o ordenamento jurídico brasileiro necessitasse de uma nova legislação que disciplinasse de maneira mais abrangente a proteção e o tratamento de dados.

O Marco Civil da Internet trouxe um efeito balizador a respeito dos direitos fundamentais na Internet no Brasil e serviu como um guia para a nova Regulação. Durante o projeto de lei elaborado para sua propositura, em meio aos escândalos de espionagem após revelações feitas por Edward Snowden, vários dispositivos sobre a tutela da privacidade foram incluídos (SOUZA; LEMOS; BOTINO, 2017, p. 88).

No dia 14 de agosto de 2018, entrou em vigor a Lei Geral de Proteção de Dados no Brasil, inspirada no Regulamento Geral de Proteção de Dados da União Europeia (RGPD). Ela “dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”.

A LGPD entrou em vigor em setembro de 2020, 24 meses após sua sanção, em virtude da Medida Provisória nº 869 de 27 de dezembro de 2018, que a alterou e acrescentou dispositivos. Ela estabeleceu diretrizes e obrigações para empresas, organizações e órgãos governamentais que lidam com dados pessoais. O que por sua vez representou um grande progresso na tutela do direito fundamental à proteção de dados consubstanciado na era da tecnologia da informação.

É imprescindível mencionar que foi promulgada a Emenda Constitucional nº 115, em 10 de fevereiro de 2022, que incluiu a proteção de dados pessoais entre os direitos e garantias fundamentais e fixou a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

A EC 115 teve origem na Proposta de Emenda à Constituição (PEC) 17/2019, aprovada pelo Senado em outubro de 2021. Apresentada pelo senador Eduardo Gomes (MDB-TO) e relatada pela senadora Simone Tebet (MDB-MS), a PEC atribui à União as competências de organizar e fiscalizar a proteção e o tratamento de dados pessoais, de acordo com a Lei Geral de Proteção de Dados (BRASIL, 2022).

O cenário histórico destacado acima evidencia a gradativa evolução do direito à privacidade. Tem-se o reconhecimento deste no âmbito internacional, e, logo após, no ordenamento jurídico de cada Estado nacional, tanto por meio de leis, como da jurisprudência.

Houve uma rápida evolução do direito à privacidade, especialmente em razão do processo de globalização. Este, além de ser uma garantia reconhecida em âmbito

internacional, passou a ser incorporado no ordenamento jurídico dos países, à exemplo do Brasil, como já citado. Entretanto, há de se considerar que ainda há muito o que prosperar, especialmente no que tange à privacidade nos meios digitais com a captação e monetização dos dados, a nova matéria-prima do século, o que também evidencia a imprescindibilidade de uma maior tutela desse direito.

2.3 A SOCIEDADE DA INFORMAÇÃO

Na atualidade, uma das expressões empegadas para definir o modo como a tecnologia impacta nossas vidas, é a noção de “sociedade da informação”. Esse termo surgiu com o intuito de substituir o conceito de “sociedade pós-industrial” e busca exprimir como as transformações tecnológicas, especialmente através da expansão do capitalismo, alteraram a nova conjuntura social. Ela é caracterizada pelo acesso amplificado à informação.

No último século, a sociedade passou por inúmeras alterações originadas pela estreita ligação do homem com a tecnologia, ampliando a forma com que se dissemina conhecimento. As Tecnologias da Informação e Comunicação – TIC, como a internet, dispositivos móveis (smartphones) e redes sociais, possibilitaram que indivíduos obtenham informações de forma rápida e abrangente, independentemente da sua localização geográfica, o que permite uma conectividade global.

Frise-se que a expressão sociedade da informação é entendida no contexto dessa sociedade pós-industrial, no que ela representa de qualitativamente relacionado à informação. Isso significa que não engloba toda a sociedade contemporânea, na medida em que muitas regiões e populações estão hoje excluídas do ambiente informacional, mas sim aquele setor dominante do mundo globalizado, o qual se caracteriza pela informação, comunicação e pelo domínio da tecnologia de ponta (SIQUEIRA JUNIOR, 2012, p. 238).

Em verdade, o processo de globalização passou a ganhar novos contornos com o advento da sociedade da informação e o desenvolvimento abrupto da tecnologia. O que antes ocorria de forma gradativa, atualmente acontece instantaneamente. Estar-se-á diante de uma avalanche de informações que são disseminadas a cada segundo e, a cada dia que passa, ganham maior importância no cenário econômico mundial.

De acordo com Manuel Castells (2001, p. 51), sociólogo e professor universitário espanhol, esse novo paradigma possui algumas características: 1) a informação é a matéria-prima; os efeitos das novas tecnologias têm alta penetrabilidade; 2) há o predomínio da lógica de redes; 3) existe uma alta flexibilidade provocada pela possibilidade de modificação e reorganização dos componentes que a integram; 4) por fim, há também uma crescente convergência de tecnologias.

A comunicação em rede transcende fronteiras, a sociedade em rede é global, é baseada em redes globais. Então, a sua lógica chega a países de todo o planeta e difunde-se através do poder integrado nas redes globais de capital, bens, serviços, comunicação, informação, ciência e tecnologia. Aquilo a que chamamos globalização é outra maneira de nos referirmos à sociedade em rede, ainda que de forma mais descritiva e menos analítica do que o conceito de sociedade em rede implica (CASTELLS, 2006, p. 18).

Porém, como as redes são seletivas, de acordo com os seus programas específicos, e porque conseguem, simultaneamente, comunicar e não comunicar, a sociedade em rede difunde-se por todo o mundo, mas não inclui todas as pessoas. Para o autor, “de facto, neste início de século, ela exclui a maior parte da humanidade, embora toda a humanidade seja afectada pela sua lógica, e pelas relações de poder que interagem nas redes globais da organização social” (IBIDEM, 2006, p. 18).

A sociedade pós-industrial, claro, é uma sociedade do conhecimento, em dois sentidos: primeiro, as fontes de inovações decorrem cada vez mais da pesquisa e do desenvolvimento (mais diretamente, existe um novo relacionamento entre a Ciência e a tecnologia, em virtude da centralidade do conhecimento teórico); segundo, o peso da sociedade, incide cada vez mais no campo do conhecimento (BELL, 1973, p.241).

Pierry Levy afirma que a quantidade bruta de dados disponíveis se multiplica e se acelera.

> A densidade dos links entre informações aumenta vertiginosamente nos bancos de dados, nos hipertextos e nas redes. Os contatos transversais entre os indivíduos proliferam de forma anárquica. É o transbordamento caótico de informações, a inundação de dados [...] (LEVY, 1999, p. 13).

De acordo com Simões (2009, p. 1), a Sociedade da Informação caracteriza-se como um novo conceito histórico no qual o fundamento das relações é estabelecido por meio da informação e da sua capacidade de transformar-se em conhecimento.

Além disso, esse conhecimento é capaz de proporcionar muitas inovações tecnológicas que são concebidas para facilitar a vida do ser humano.

O desenvolvimento do capitalismo ao longo do século XX, aliado ao crescimento do progresso tecnológico, dá uma maior ênfase à informação. A utilização massiva de TICs, que tem por consequência a distribuição de informação, alteraram os diversos âmbitos da sociedade. Surge, então, uma nova configuração social, econômica e política: a sociedade da informação. Uma de suas principais características é a facilidade exorbitante na coleta, processamento, armazenamento e transmissão de dados, especialmente no meio digital.

As máquinas passam a integrar o cotidiano das pessoas e alteraram de forma significativa as relações humanas, tanto no setor público, quanto no privado. Elas geram uma certa “comodidade” e fazem com que grande parte dos usuários passassem a não se importar de forma habitual com a possibilidade de terem seus dados coletados e usados como matéria-prima das empresas. Em verdade, é possível observar que a praticidade aliada a falta de informação acerca do funcionamento das TICs é um grande alimento para que a privacidade seja violada.

Como se percebe, os avanços da tecnologia são surpreendentes e capazes de criar um novo universo de relações, especialmente consideradas a partir do referencial da sociedade digital ou da informação, em que os dados são vistos como o “novo petróleo”, isto é, são a principal matéria-prima em ascensão na sociedade da informação. Acentuadamente, cada vez mais, a pessoa humana se encontra na dependência dos meios de eletrônicos, onde o trânsito de suas informações pessoais (autorizadas e não autorizadas) a expõe a constantes riscos (BITTAR, 2003 p. 279).

O surgimento do termo “Sociedade da Informação” se deu na década de 1970, especialmente no Japão e Estados Unidos da América (EUA), no âmbito de discussões sobre o que seria a “sociedade pós-industrial”, bem como quais seriam suas principais características (TAKAHASHI, 2000, p.2).

Em 1993, se utilizou pela primeira vez de forma oficial a expressão “sociedade da informação” pelo então presidente da Comissão Europeia, Jacques Delors, no Conselho da Europa de Copenhague, para definir o crescente uso da tecnologia da informação, no intuito de reforçar a economia, melhorar a prestação dos serviços públicos e incrementar a qualidade de vida dos cidadãos (MARTINS, 2000, p. 43).

A definição mais comum de Sociedade da Informação enfatiza as inovações tecnológicas. A ideia chave é que os avanços no processamento, recuperação e

transmissão da informação permitiram aplicação das tecnologias de informação em todos os cantos da sociedade, devido a redução dos custos dos computadores, seu aumento prodigioso de capacidade de memória, e sua aplicação em todo e qualquer lugar, a partir da convergência e imbricação da computação e das telecomunicações (GIANNASI, 1999, p.21).

Depreende-se que no presente e futuro, a principal matéria utilizada no capitalismo digital é a informação. Trata-se de uma verdadeira revolução, comparada com a Revolução Industrial do século XVIII, no entanto, com uma dimensão muito maior. De acordo com Castells (2003, p. 67) um aspecto adicional que se levanta em relação à revolução da tecnologia da informação é que, ao contrário das demais revoluções, que ocorreram em uma área geográfica limitada do planeta, com lenta expansão para outras regiões, esta revolução se difundiu celeremente por todo o globo em menos de duas décadas.

A partir de então, a sociedade passa a ser caracterizada pelo fortalecimento das tecnologias em todos os âmbitos da vida social. De forma ampla, desde à economia, política até a educação. Nesse sentido, se torna imprescindível uma análise acerca de como a tecnologia capta a matéria-prima (informação), como as utiliza e qual a finalidade, tendo como principal premissa o direito à privacidade.

Essa nova capacidade de tratamento de dados permite a identificação de tendências, não mais baseadas em amostragens, mas no processamento da universalidade dos dados. Deste modo, aumenta a precisão e as possibilidades de resultados a serem obtidos, permitindo, dentre outros resultados, identificar padrões de consumo, conforme o comportamento de compra dos consumidores, sua localização (e.g. as discutidas técnicas de *geopricing*, pelas quais a determinação do preço de produtos ou serviços se dá conforme o lugar em que esteja o consumidor), a interação em redes sociais, ou a personalização da negociação com consumidores mediante uso de regras pré-determinadas ou de inteligência artificial (MIRAGEM, 2019, p. 2).

Computadores e tecnologia de informação proveem uma infraestrutura que possibilita o processamento e a distribuição da informação, permitindo o seu manuseio numa escala sem precedentes históricos, facilitando as relações de comércio em tempo real numa escala global. Tem sido excepcionalmente rápido o crescimento do setor comercial da informação na economia, ressaltando o crescimento explosivo de

serviços, tais como os meios de comunicação de massa (transmissão por satélite, cabo, vídeo) e as bases de dados on-line (GIANNASI, 1999, p. 24).

O anseio pela comercialização de informações se intensifica ainda mais quando a economia migra para a internet, especialmente quando se fala em "*big techs*", isto é, grandes empresas do ramo da tecnologia. O marketing operado por essas empresas faz com que os consumidores que já tiveram suas informações captadas e tratadas, sejam induzidos a comprar determinado produto. Trata-se de uma verdadeira violação ao direito à privacidade e liberdade dos indivíduos, que carece de regulamentação eficaz na seara jurídica.

O capitalismo não entregou os bens às pessoas; as pessoas foram crescentemente entregues aos bens; o que quer dizer que o próprio caráter e sensibilidade das pessoas foi reelaborado, reformulado, de forma tal que elas se agrupam aproximadamente com as mercadorias, experiências e sensações, cuja venda é o que dá forma e significado a suas vidas (SEABROOK, 1988, p.183).

A informação se tornou um produto valioso e, seu rápido acesso e compartilhamento passaram a ser imprescindíveis para o desenvolvimento de atividades econômicas, sociais e políticas. Entretanto, essa nova ordem também apresenta desafios e questões complexas. A fartura no compartilhamento de informações pode fazer com que a privacidade e a segurança dos dados sejam expostas, visto que é necessário que a coleta e o uso dessa nova matéria-prima sejam realizados de forma ética e responsável, além de haver respeito à legislação vigente, o que não acontece em grande parte dos casos.

3 A NECESSIDADE DE PROTEÇÃO DE DADOS FRENTE AO CAPITALISMO DE VIGILÂNCIA OPERADO PELAS BIG TECHS

O presente capítulo versa sobre o capitalismo de vigilância sob uma ótica negativa da monetização de dados, no intuito de encontrar o momento em que a competitividade das grandes empresas (as *big techs*) provocou uma mudança no comportamento das máquinas, de modo que elas desenvolveram meios de conhecer os comportamentos humanos e a partir disso molda-los para um fim específico. Em seguida, descreveu-se acerca do protagonismo das *big techs* na sociedade da informação**.** Por fim, foi necessário dissertar sobre a norma europeia que inspirou a criação da Lei Geral de Proteção de Dados no Brasil, qual seja, o Regulamento Geral de Proteção de Dados (RGPD).

3.1 MONETIZAÇÃO DE DADOS: UMA ABORDAGEM CONCEITUAL ACERCA DO CAPITALISMO DE VIGILÂNCIA

Atualmente, o crescimento exponencial do meio digital é uma realidade que não pode ser ignorada. No entanto, na medida em que esse avanço é visto como positivo, uma vez que promove o acesso à informação, por outro lado, também impulsiona um dever estatal de proteção, especialmente no que concerne à direitos fundamentais como a privacidade e proteção de dados.

No último século, a sociedade passou por inúmeras alterações originadas pela estreita ligação do homem com a tecnologia, ampliando a forma com que se dissemina conhecimento. As Tecnologias da Informação e Comunicação – TIC, como a internet, dispositivos móveis (smartphones) e redes sociais, possibilitaram que indivíduos obtenham informações de forma rápida e abrangente, independentemente da sua localização geográfica, o que permite uma conectividade global.

Estar-se-á diante de uma nova conjuntura social, interconectada pela comunicação e pela disseminação de informações globalizadas, caracterizada pela mercantilização de dados. De acordo com Pierry Levy (1999, p. 46), tem-se um espaço de comunicação que vem crescendo com a ampliação de um movimento internacional de pessoas ávidas para experimentar, coletivamente, formas de comunicação

diferentes daquelas que as mídias clássicas nos propõem. Ou seja, o ciberespaço é o novo meio de comunicação que surge da interconexão mundial dos computadores.

A internet, que antes era apenas uma vasta área de oportunidades e possibilidades a serem conhecidas, passou a ser interpretada como uma “nova era”. Ou melhor, deixou de ser um mero instrumento de comunicação entre pessoas, para ter uma própria independência estrutural, que utiliza dados de indivíduos com o objetivo de construir padrões de comportamento e pensamento entre sujeitos. Essa captação e movimentação de dados é chamada de capitalismo de vigilância. O termo foi popularizado por Shoshana Zuboff, professora emérita da Harvard Business School, em seu livro "The Age of Surveillance Capitalism" (A Era do Capitalismo de Vigilância), publicado em 2019.

De acordo com Shoshana Zuboff (2021, p. 22) o capitalismo de vigilância reivindica de maneira unilateral a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais. Ainda segundo as lições da autora supramencionada, embora alguns desses dados sejam aplicados para o aprimoramento de produtos e serviços, o restante é declarado como *superávit* comportamental do proprietário, alimentando avançados processos de fabricação conhecidos como “inteligência de máquina”; e manufaturados em produtos de predição que antecipam o que um determinado indivíduo faria agora, daqui a pouco e mais tarde. (ZUBOFF, 2021, p. 22)

O desenvolvimento do capitalismo ao longo do século XX, aliado ao crescimento do progresso tecnológico, dá uma maior ênfase à informação. A ascensão das *big techs*, aliadas com as TICs e algoritmos, sequência finita de passos bem definidos e ordenados que visam resolver problemas e realizar tarefas, que tem por consequência a distribuição de informação, alteraram os diversos âmbitos da sociedade. Surge, então, uma nova configuração social, econômica e política: a sociedade da informação. Uma de suas principais características é a facilidade exorbitante na coleta, processamento, armazenamento e transmissão de dados, especialmente no meio digital.

O mercado baseado na economia de dados fez com que a competitividade exacerbada provocasse mudança no comportamento das tecnologias, de modo que elas desenvolveram meios de “entender” os comportamentos humanos através da captação de dados e a partir disso contorna-los para um fim determinado. Desse modo, o processo de globalização passou a ganhar novos contornos com o advento

da sociedade da informação e o desenvolvimento abrupto da tecnologia. O que antes ocorria de forma gradativa, atualmente acontece instantaneamente. Estar-se-á diante de uma avalanche de informações que são disseminadas a cada segundo e, a cada dia que passa, ganham maior importância no cenário econômico mundial.

De acordo com Manuel Castells (2001, p. 51), sociólogo e professor universitário espanhol, esse novo paradigma possui algumas características: 1) a informação é a matéria-prima; os efeitos das novas tecnologias têm alta penetrabilidade; 2) há o predomínio da lógica de redes; 3) existe uma alta flexibilidade provocada pela possibilidade de modificação e reorganização dos componentes que a integram; 4) por fim, há também uma crescente convergência de tecnologias.

A professora Zuboff (2021, p. 23) afirma que o capitalismo de vigilância gera uma nova espécie de poder que chama de instrumentarismo. O referido poder, recém nomeado de instrumentário, conhece e molda o comportamento humano em prol das finalidades de terceiros. Esse poder sobre o comportamento humano está relacionado não só com a ideia da prática consumista, mas também com a utilização das tecnologias digitais com fito interferir em processos democráticos, como na escolha do voto, por exemplo.

O fenômeno do capitalismo de vigilância se refere a uma mutação do capitalismo da informação, ou seja, a partir da expansão das tecnologias digitais decorrentes do modelo de sucesso dos produtos da Apple, no início dos anos 2000, e pelas grandes empresas de tecnologia do Vale do Silício, surgiram no final do século XX as condições necessárias para uma chamada terceira modernidade, a qual estava voltada para o indivíduo, tendo como foco a realização dos valores e expectativas do sujeito (ZUBOFF, 2020).

A vigilância é um aspecto cada vez mais presente nas notícias diárias, o que reflete sua crescente importância em muitas esferas da vida. Mas, na verdade, a vigilância tem se expandido silenciosamente por muitas décadas e é uma característica básica do mundo moderno. À medida que esse mundo vem se transformando ao longo de sucessivas gerações, a vigilância assume características sempre em mutação (BAUMAN, 2013, p. 7).

Nesse contexto, as máquinas passam a integrar o cotidiano das pessoas e alteraram de forma significativa as relações humanas, tanto no setor público, quanto no privado. Elas geram uma certa “comodidade” e fazem com que grande parte dos usuários passassem a não se importar de forma habitual com a possibilidade de terem

seus dados coletados e usados como matéria-prima das empresas. Em verdade, é possível observar que a praticidade aliada a falta de informação acerca do funcionamento das TICs é um grande alimento para que a privacidade seja violada.

Como se percebe, os avanços da tecnologia são surpreendentes e capazes de criar um novo universo de relações, especialmente consideradas a partir do referencial da sociedade digital ou da informação, em que os dados são vistos como o “novo petróleo”, isto é, são a principal matéria-prima em ascensão na sociedade da informação. Acentuadamente, cada vez mais, a pessoa humana se encontra na dependência dos meios de eletrônicos, onde o trânsito de suas informações pessoais (autorizadas e não autorizadas) a expõe a constantes riscos (BITTAR, 2015, p. 279).

O sociólogo Christian Fuchs (2013, p. 272) aduz que a mercantilização de dados acontece da seguinte forma: empresas de tecnologia investem dinheiro na estrutura tecnológica e em trabalhadores que produzirão serviços de social media que serão disponibilizados gratuitamente para os usuários, que por sua vez utilizarão essas plataformas para gerar conteúdo, aprimorando-as. O produto final é o conjunto de dados pessoais gerados a partir de uma série de operações sobre o comportamento online, que será vendido como uma commodity para o setor de publicidade num preço maior do que o investido inicialmente.

Há diversas formas de manipular os dados, a depender do objetivo que se pretende alcançar. A lógica é que a extração de informações através do uso das plataformas seja utilizada para captar padrões de comportamentos dos indivíduos e, a partir disso, moldar técnicas algorítmicas de persuasão, uma vez que há a previsibilidade de determinada tomada de posição de forma antecipada.

Evangelista (2017, p. 247) descreve que, por exemplo, imaginemos um plano de saúde, que, como condição para oferecer preços mais baixos, oferte ao cliente o uso ininterrupto de uma pulseira de monitoramento cardíaco. Antes, a empresa podia apenas recomendar ao cliente que se exercitasse três vezes por semanas por pelo menos 30 minutos ao dia para manter uma vida saudável pelo seu próprio bem.

Com a pulseira, a sincronizar dados com os computadores da empresa diariamente, esta tem como estar certa de como o cliente se comportou, se fez exercícios ou não, verificando os batimentos cardíacos. Se o cliente não cumpriu o “recomendado” então os preços, automaticamente, sobem. O risco da empresa cai consideravelmente, pois dá preços mais altos aos sedentários, condição que ela

verifica ao vigiar a que velocidade bate o coração do segurado (EVANGELISTA, 2017, p. 247).

Verifica-se uma espécie de “publicidade predatória”. Os algoritmos exercem uma verdadeira vigilância na predileção das pessoas, com o objetivo de identificar suas necessidades e pensamentos através da captação de dados no momento em que o usuário acessa a rede. É possível que um indivíduo pesquise um modelo de um tênis, por exemplo, e logo após, surjam inúmeros anúncios acerca do produto.

O’Neill (2016, pp. 64-65) afirma que os algoritmos podem identificar contextos de vulnerabilidade para estabelecer políticas de lucro sobre elas. Assim, se um indivíduo está desesperadamente endividado ou sem dinheiro, surgirão anúncios de ofertas de empréstimos com altíssimas taxas de juros. Na educação, é oferecida uma falsa estrada para a prosperidade ao mesmo tempo em que as empresas do ramo calculam como maximizar sua receita a partir de cada caso, num loop de empréstimos e dívidas, sem que o consumidor sequer saiba como determinado anúncio chegou a ele.

Ainda não se sabe a forma exata com que os dados são usados, capturados e fornecidos por meio de algoritmos, com o objetivo de alavancar a venda de produtos. O que se tem conhecimento é que isso acontece de forma recorrente durante a navegação de sites, especialmente nas *big techs*, pioneiras nesse negócio. Essa prática traz à baila demandas éticas e preocupações sobre a privacidade e a proteção de dados, tendo em vista que diversas vezes o usuário não está ciente da amplitude da coleta e do uso de seus dados.

No entanto, Finkelstein e Finkelstein (2019, p. 291) explicam que esse “perigo” se materializou em março de 2018, quando veio a público o escândalo da *Cambridge Analityca* (CA), empresa britânica que se mostrou apta a analisar imensa quantidade de material e dados combinando-os com ciência comportamental, visando identificar pessoas e empresas que poderiam ser contatadas via envio de material de marketing, ou mesmo influenciando campanhas políticas e eleições presidenciais. A CA, sem autorização expressa e sem publicar tais resultados, coletava dados de diversas fontes, mas principalmente de plataformas de mídia social, como o *Facebook*.

Nota-se que a vigilância é um aspecto cada vez mais presente nas notícias diárias, o que reflete sua crescente importância em muitas esferas da vida. Mas, na verdade, a vigilância tem se expandido silenciosamente por muitas décadas e, é uma característica básica do mundo moderno. À medida que esse mundo vem se

transformando ao longo de sucessivas gerações, a vigilância assume características sempre em mutação. Hoje, as sociedades modernas parecem tão fluidas que faz sentido imaginar que elas estejam numa fase “líquida”. Sempre em movimento, mas muitas vezes carecendo de certezas e de vínculos duráveis, os atuais cidadãos, trabalhadores, consumidores e viajantes também descobrem que seus movimentos são monitorados, acompanhados e observados. A vigilância se insinua em estado líquido. (BAUMAN, 2013, p. 7).

O fenômeno da vigilância atualmente se distingue das formas tradicionais de controle social, pois a tecnologia possibilita a coleta, armazenamento, processamento, classificação e transmissão de informações numa dimensão nunca sequer imaginada. Portanto, não se trata apenas de uma “versão eletrônica da vigilância”, mas de um fenômeno qualitativamente novo que transcende a distância, a escuridão, o tempo e as barreiras físicas. (BAUMAN, 2013, p. 8).

Yuval Harari (2018, p. 83) ensina que quando a autoridade passa de humanos para algoritmos, não podemos mais ver o mundo como o campo de ação de indivíduos autônomos esforçando-se por fazer as escolhas certas. Em vez disso, observa-se o universo inteiro como um fluxo de dados, considerar organismos pouco mais que algoritmos bioquímicos e acreditar que a vocação cósmica da humanidade é criar um sistema universal de processamento de dados – e depois fundir-se a ele. Já estamos nos tornando, hoje em dia, minúsculos chips dentro de um gigantesco sistema de processamento de dados que ninguém compreende a fundo.

Essa conjuntura se tornou um imbróglio quando a competitividade provocou mudança no comportamento das máquinas, de modo que, ao serem “alimentadas” de informações, elas desenvolveram meios de conhecer os comportamentos humanos através de algoritmos e a partir disso molda-los para um fim específico. O fim que elas pretendem, na maioria das vezes, está relacionado ao lucro, já que a captação de informações através das *big techs* é empregada para verificar padrões de comportamentos dos usuários e, a partir dessa concepção, molda procedimentos algorítmicos de influência, fazendo com que haja uma grande previsibilidade de tomada de decisão de forma antecipada.

Uma das grandes problemáticas, de acordo com Frazão (2019, p. 04) é o excesso de otimismo das próprias pessoas com relação a muitos dos modelos de negócios da economia digital e os benefícios diretos que eles lhes proporcionam. Aliada às próprias dificuldades de compreensão dos seus efetivos impactos, são

também fatores que criam ônus adicionais para os reguladores que, premidos entre a assimetria informacional e os benefícios das inovações, muitas vezes não sabem o que fazer para conter esse processo e proteger minimamente os cidadãos. É esse o cenário que possibilitou que vários desses negócios evoluíssem em um ambiente no qual o suposto vácuo regulatório foi convenientemente preenchido pela autorregulação criada pelos próprios agentes em seu benefício.

Os avanços tecnológicos estão cada vez mais presentes na vida das pessoas. Inerente a isso, percebe-se uma maior amplitude nas funcionalidades oferecidas pelo meio digital. Essa facilidade em realizar ações com “um click” gera nos indivíduos um certo “conforto” em aceitar tudo que a rede dispõe sem analisar os riscos a ela inerentes. Nesse sentido, o capitalismo de vigilância pode ser entendido como o problema do século, pois ele levanta inúmeras questões que precisam ser discutidas, no que tange à mercantilização de dados e suas consequências para a sociedade.

3.2 O PROTAGONISMO DAS BIG TECHS NA SOCIEDADE DA INFORMAÇÃO

O surgimento da sociedade da informação, caracterizada pela amplificação do uso das ferramentas digitais para o armazenamento de dados, facilitou o descobrimento de bases pessoais, tendo como consequência, inúmeros casos de vazamentos de informações sigilosas, especialmente quando se trata de grandes empresas que dominam o meio digital, as denominadas *big techs*. Essas pessoas jurídicas, atualmente, são consideradas líderes em seus respectivos seguimentos e por manusearem dados, a nova matéria-prima do século XXI, passaram a ter uma enorme influência na economia, política e sociedade em todo o mundo.

O emergente crescimento da tecnologia digital refletiu na expansão dessas empresas, ou melhor, um novo modelo de negócios baseado na “economia de dados”. Junto a isso, a sociedade também se modificou, especialmente no que se refere à defesa dos direitos e garantias fundamentais frente à evolução tecnológica, uma vez que, como se sabe, o digital traz inúmeras ameaças e preocupações. Por isso, houve a necessidade de uma legislação que abarcasse todas essas problemáticas inerentes ao ciberespaço.

Em se tratando de conceito das *big techs*, Stegmann (2020, p. 52) afirma que o termo *tech*, ao contrário do senso comum, não se refere necessariamente às empresas de tecnologia, mas, sim, àquelas que são parte ativa na evolução de

determinado mercado. Com o desenvolvimento de novos produtos e tecnologias, essas companhias acabam por criar e pavimentar caminhos para que outros agentes do mercado se estabeleçam ou, ainda, de modo a alterar profunda e estruturalmente o próprio mercado em exame.

Quanto ao termo *big*, também não necessariamente se refere à posição no ranking econômico do setor, mas, sim às seguintes características, que são mais comuns e acentuadas entre as *big techs*, permitindo que sejam identificadas como as verdadeiras gigantes do mercado em apreciação. Para atingir o nível de *big tech*, além de fomentar a criação de tecnologias únicas e de difícil replicação, podemos constatar: (i) Grande valor de mercado; (ii) Operabilidade em diversos mercados e criação de um ecossistema entre eles; e (iii) Protagonistas em mudanças sociais (ZUQUIM, 2021, p. 15).

As *big techs* são conhecidas pela sua grandiosidade relacionada ao poder econômico, mas não se restringem a isso. Sua mais importante característica está atrelada à dominação do mercado mundial. O que antes era adstrito à uma região, passou a ultrapassar fronteiras. Elas são os verdadeiros monopólios ou oligopólios do mercado digital, com o diferencial de serem detentoras das inovações tecnológicas e produtos disruptivos.

O comércio não é mais local, é global. A burguesia contemporânea é composta por empresas que atuam em todo o mundo e não têm suas fronteiras dentro de um Estado, circulam com seus produtos em vários Estados. Da mesma forma que na baixa Idade Média, precisa-se de regras, previsíveis que possibilitem modelos de negócios aplicáveis em todo o mundo, com sistemas de solução de controvérsias que protejam seus investimentos. Para isso, é necessário criar estruturas globais de produção, execução e aplicação das regras jurídicas (VARELLA, 2013, p. 79).

As *big techs*, são, portanto, os centros de uma complexa teia de relações empresariais e não empresariais, cujo poder precisa ser adequadamente compreendido diante desse contexto de interconexão, bem como dos seus relevantes efeitos de rede. Dessa maneira, o número de conexões, bem como a sua variedade e sofisticação, precisam ser considerados pela autoridade antitruste, ainda mais diante do fato de que as plataformas são capazes de extrair vantagens de todos os usuários que dependam da sua infraestrutura, inclusive para efeitos de limitar a possibilidade de determinados agentes econômicos de buscar seus usuários de forma independente (FRAZÃO, 2018, p. 07)

É inegável que o mercado digital dominou a economia mundial. A grande predisposição de concentração de capital e poder nas “mãos” de uma minoria faz com que haja a dominação de determinados mercados, como os de publicidade e busca. À título de exemplo, cita-se a atuação de empresas como *Amazon*, *Apple*, *Google*, *Facebook (Meta Platforms Inc.)* e *Microsoft*.

Assim como acontece na cadeia consumerista, é perceptível que o usuário, aqui também considerado como consumidor, se encontra em uma posição de vulnerabilidade, especialmente diante da não regulação dessas empresas. O ato de acessar uma plataforma a aceitar os termos de uso faz com que o titular disponibilize seus dados para as *big techs*, que, por seu turno, se acobertam por trás de uma falsa ideia de consentimento e utilizam essas informações como matéria-prima para formar opiniões através das predileções extraídas.

Nesse contexto, as *big techs*, através do uso de algoritmos e inteligência artificial, reúnem e selecionam as informações fragmentadas da web,

> [...] de modo a fazer predições comportamentais e influenciar a formação de opiniões, valores e processos de tomada de decisão, [...] promovem uma sociabilidade induzida por algoritmos que visam reter o máximo da atenção diária de usuários em todo mundo (MACHADO; MISKOLCIP, 2019, pp. 946-952).

Pode-se afirmar que essa é uma nova maneira de uniformizar pensamentos e coibir dissensos, onde “a seleção de conteúdo a partir de sua ‘viralização’ tende a favorecer uma diversidade pobre de temáticas em vez de um pluralismo positivo e democratizante”, que também contribui para disseminação de *fake news* (*IBIDEM*, 2019, p. 947).

A problemática central da ascensão das *big techs* no mercado digital está fundada na impossibilidade dos indivíduos contarem com a clareza dos contratos (termos de uso de privacidade e cookies), tornando evidente o desamparo do titular de dados que acessa as ferramentas disponibilizadas no ciberespaço. Em consequência disso, inúmeros são os casos de violação de direitos fundamentais imprescindíveis ao ser humano, como a privacidade e proteção de dados, já que eles são colocados em risco em prol da dominação e influência de grandes empresas que faturam com a manipulação de informações. A partir disso surge a imprescindibilidade de uma regulação responsiva.

Diante desse imbróglio, discussões sobre a necessidade de regulação das *big techs* estão no centro das atenções há alguns anos. No entanto, foi em 2018 que veio à tona o escândalo em que o *Facebook*, através da ação da *Cambridge Analytica*, teria vazado dados para serem utilizados para influenciar a opinião de eleitores em diversos países do mundo em meio a campanhas políticas. Com isso, verificou-se o grande poder dessas empresas e alguns estudiosos passaram a questionar qual o papel do Estado diante desse cenário (SILVA, 2022, p. 01).

O novo contexto fomentado pelas tecnologias fez com que houvesse a necessidade do legislador positivar leis que resguardassem direitos que até então não eram vistos como imprescindíveis, já que algumas décadas atrás o ciberespaço era uma ideia afastada da realidade da época. No Brasil, em 23 de abril de 2014, foi publicada a Lei nº 12.965/2014, conhecida como “Marco Civil da Internet”. Ela estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Já no mês de agosto de 2020, inspirada no Regulamento Geral de Proteção de Dados da União Europeia (*General Data Protection Regulation*) – RGPD, entrou em vigor a Lei Geral de Proteção de Dados Pessoais (LGPD) (Lei nº 13.079/18), com o objetivo de proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Com relação aos dados, cita-se a Emenda Constitucional nº 115 de 10 de fevereiro de 2022, que incluiu a proteção de dados pessoais entre os direitos e garantias fundamentais e fixou a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Essas são as legislações, apesar de significarem um grande avanço na tutela de direitos no mundo digital, ainda estão longe de ser uma solução para os imbróglios nela existentes.

No tocante a disseminação de informações falsas, cita-se o Projeto de Lei n. 2630/2020 (mais conhecido como PL das *Fake News*), de iniciativa do Senador Alessandro Vieira do partido Cidadania/SE, dispõe sobre um novo formato de regulamentação e fiscalização de plataformas digitais. A PL “estabelece normas relativas à transparência de redes sociais e de serviços de mensagens privadas, sobretudo no tocante à responsabilidade dos provedores pelo combate à desinformação e pelo aumento da transparência na internet, à transparência em relação a conteúdos patrocinados e à atuação do poder público, bem como estabelece sanções para o descumprimento da lei” (Brasil, 2020).

No entanto, as grandes empresas de tecnologia (*Google*, *Amazon*, *Facebook*...) entendem que a proposta supramencionada apresenta um viés antidemocrático, pautado na violação da liberdade de expressão, considerada aqui como “a possibilidade de legitimação de sensibilidades discordantes, vozes em dissenso, visões menos monocolores e menos subservientes ao poder político” (BORGES, 2016, p. 368). Nesse sentido, é inegável que as questões de direitos humanos estão no pilar dessa discussão, especialmente no que se refere à uma possível violação à privacidade e proteção de dados, em virtude dos inúmeros casos de informações falsas (*fake news*) disseminadas através de perfis revestidos de anonimato, que podem moldar a formação de opinião do cidadão através da captura de predileções e lançamento de informações na rede através do algoritmo e inteligência artificial.

É inegável que a revolução digital é uma grande questão global de direitos humanos, sendo necessário considerar que seus inquestionáveis benefícios não anulam seus riscos inconfundíveis (OHCHR, 2019, p. 54). Atualmente, os dados pessoais têm sido utilizados por governos e grandes players econômicos para a criação de um *one way mirror*, possibilitando que tais agentes saibam tudo dos cidadãos, enquanto estes nada sabem dos primeiros. E tudo isso acontece por meio de um monitoramento e vigília constantes sobre cada passo da vida das pessoas, o que leva a um verdadeiro capitalismo de vigilância, cuja principal consequência é a constituição de uma sociedade também de vigilância (PASQUALE, 2015, pp. 9-45).

O que acontece é que em plataformas como o *Google*, *Facebook* e *Amazon*, os usuários não são cobrados para utilizar os serviços porque são a fonte de abastecimento de dados. Diferente do “mundo real”, em que os indivíduos escolhem o que querem consumir, no “mundo virtual” as pessoas são induzidas massivamente a consumir o que as plataformas desejam, com fito de influenciar o usuário a adquirir algum produto ou até mesmo de ratificar determinadas ideologias por meio de notícias falsas, disseminadas através do uso de tecnologias.

Diante de tal disfuncionalidade que a operacionalização dos algoritmos e inteligência artificial como fragmentadores de realidades proporciona, a regulação das *big techs* se apresentam como uma proposta que visa alcançar um ambiente informativo mais confiável, no qual será possível inovar e reconstruir o peso dos indivíduos e das comunidades na seleção dos conteúdos (BEIRIZ; et. al., 2021, p. 03).

Logo, as medidas estatais devem ser reflexas no sentido de não só preservar o núcleo da liberdade de expressão e informação, mas de garantir que os usuários tenham os direitos à privacidade e proteção de dados resguardados. Yuval Harari (2018, pp. 111-112) cita que a regulação da propriedade de dados é talvez a questão política mais importante da nossa era e, se não formos capazes de dar respostas para esse problema, nosso sistema sociopolítico poderá entrar em colapso.

Por outro lado, Frazão (2018, p. 03) entende que a regulação do tratamento de dados pessoais é tema de extrema complexidade e requer, para a sua solução satisfatória, várias iniciativas além das jurídicas. Mesmo no âmbito do direito, não há respostas lineares, pois, diante da existência de leis gerais de proteção de dados, como é o caso da Lei Geral de Proteção de Dados - LGPD brasileira, indaga-se em que medida tal regulação, sozinha, poderá ter plena eficácia ou se outras áreas, não deveriam também endereçar aspectos do problema, desde que estes, obviamente, sejam compatíveis com suas finalidades e com a harmonia e a unidade que se esperam do sistema como um todo.

A tendência da regulação brasileira é adotar a autorregulação regulada, ou seja, as plataformas deverão adotar regras de comportamento no seu ecossistema, com a possibilidade de caso violado algum direito, recorrer-se ao Judiciário (SANTIN; PRA, 2022, p. 15). No mesmo contexto, há opiniões contrárias à regulação. Principalmente contrárias ao modelo de regulação tradicional, onde o Estado interfere diretamente no assunto sem consultar as outras partes envolvidas. Existem alternativas melhores para o modelo tradicional: a auto-regulação — quando as empresas definem sozinhas os padrões a serem seguidos — e a regulação mista — onde sociedade e plataformas agem de maneira conjunta para melhorar o serviço prestado (BEIRIZ; et. al., 2021, p. 07). Entretanto, nenhuma delas apresenta respostas positivas e congruentes com a problemática.

Crê-se que o modelo atual – não intervir e/ou atuar apenas em casos extremos – está fadado ao fracasso, justamente pelo crescimento vertiginoso das empresas do setor. A internet mudou a estrutura do capitalismo, possibilitou a concentração global de capital nas Big Techs e, ainda, ameaça as bases da Democracia em diversos países (TAMBINI E MOORE, 2022, p. 1).

Diante disso, por analogia, uma solução viável seria a utilização da Teoria da Regulação Responsiva, desenvolvida na obra *Responsive Regulalation – Transcending the Deregulation Debate*, de Ian Ayres e John Braithwaite (1992). Nela,

entende-se que a abdicação da responsabilidade das empresas poderia ser minimizada pela participação conjunta entre empresas, governos e partes interessadas em um programa de regulamentação. Quando a empresa ajuda na composição das normas a ela aplicadas, é mais difícil que racionalize a ilegalidade. Além disso, evidências consideráveis indicam que a participação em um processo de tomada de decisão aumenta a aceitação e melhora a execução das decisões tomadas (AYRES; BRAITHWAITE, 1992, p.115).

Trata-se de uma aproximação entre o público e o privado com o objetivo de haver uma colaboração entre ambos, a consequência, é, sem dúvidas, obter um maior benefício social. A teoria da regulação responsiva pressupõe uma ação estatal mais próxima do ente regulado e contínua à procura de novas estratégias quando o regulador é confrontado com insucessos recorrentes, assumindo-se que a maior parte das iniciativas regulatórias fracassam na maioria dos contextos de aplicação (BRAITHWAITE, 2011, p. 22).

A ideia deste modelo é justamente que o legislador possa transitar em diversos níveis, tentando o caminho da persuasão enquanto for possível (v.g, no caso de infrações leves ou de o agente demonstrar um comportamento virtuoso), e recorra às sanções mais aflitivas quando se fizer necessário (SILVA, 2022, p. 05).

A informação se tornou um produto valioso e, seu rápido acesso e compartilhamento passaram a ser imprescindíveis para o desenvolvimento de atividades econômicas, sociais e políticas. Entretanto, essa nova ordem também apresenta desafios e questões complexas, como a própria imprescindibilidade de regulação. A fartura no compartilhamento de informações pode fazer com que a privacidade e a segurança dos dados sejam expostas, visto que é necessário que a coleta e o uso dessa nova matéria-prima sejam realizados de forma ética e responsável, além de haver respeito à legislação vigente, o que não acontece em grande parte dos casos.

3.3 A EXPERIÊNCIA EUROPEIA COM O REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

Nos últimos anos, a tecnologia cresceu de forma alarmante, o que resultou em uma sociedade informatizada, caracterizada pelo fluxo contínuo de dados. Isso tem resultado em uma revolução na maneira como o ser humano se relaciona com os

dispositivos de conexão em rede. Para cadastros virtuais, criação de contas em aplicativos, acesso à informação, todos os aspectos da vida dentro da estrutura social associada ao crescente fluxo informacional, a chamada sociedade em rede (CASTELLS; CARDOSO, 2005, p 03).

A informação passou a ser um produto valioso e uma nova modalidade de comércio se instaurou: a comercialização de dados. Em razão disso, a proteção de dados agora é uma preocupação a nível mundial, tendo em vista os inúmeros casos de violações de direitos fundamentais existentes. Estudos do Consumrs International (2018, p. 02) demonstram que, atualmente, já são mais de cem países com marcos regulatórios para proteção de dados pessoais em todo o mundo.

O Regulamento Geral de Proteção de Dados da União Europeia – RGPD (*General Data Protection Regulation* – GDPR 2016/679), aprovado em 2016, que entrou em vigor em 2018, após dois anos de vacância, é um exemplo de marco regulatório imprescindível para a proteção de dados. Ele substituiu a Diretiva de Proteção de Dados de 1995/46 EC (Directive Protection Data – DPD 1995/46 EC - DPD), e estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados[6].

Um dos problemas da DPD, que ensejou a necessidade de elaboração da RGPD, é que não no âmbito de todos os países de forma indiscriminada, isto é, necessitava “ser recepcionada por cada país, de acordo com suas leis nacionais para, assim, ser aplicada ao caso concreto” (LEE, 2018, p. 34). Logo, havia assimetria entre a aplicação da DPD em situações semelhantes na União Europeia, o que manifestou no legislador a ideia de necessidade de reforma, com o objetivo de garantir a uniformidade da aplicabilidade da norma em todo o território.

Assim, embora houvesse uma previsão legal, que, em linhas gerais devesse ser aplicada de maneira uniforme, o que se reproduziu de maneira fática foi uma grande variedade de leis nacionais, através das quais cada estado europeu retirava uma grande margem de discricionariedade quando da aplicação da Diretiva

[6] Artigo 1.º Objeto e objectivos

1. O presente regulamento estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
2. O presente regulamento defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais.
3. A livre circulação de dados pessoais no interior da União não é restringida nem proibida por motivos relacionados com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais.

(CAETANO, 2020, p. 06). Isso porque as diretivas carecem de transposição interna pelos Estados-Membros. Deste modo, os Estados-Membros ficaram dotados de margem de discricionariedade na sua transposição, o que originou uma transposição heterogénea nos diferentes Estados-Membros (MELO, 2019, p. 23).

Frise-se que em razão de tal disparidade legal, muitas empresas norte americanas apoiavam-se nas brechas das leis para não adotar as medidas de *compliance* (DENLEY, et al. 2018, p. 05). Isso fez com que a proteção de dados ficasse vulnerável frente as disposições legais existentes e o que motivou a criação do Regulamento Geral de Proteção de Dados - RGPD.

Em síntese, o RGPD regulamenta o direito fundamental à proteção de dados, estatuído no art. 8º da Carta Europeia de Direitos Humanos[7], cujo âmbito material de aplicação atinge aqueles que têm um arquivo automatizado contendo dados pessoais (LIMBERGER, 2022 p. 483).

Nesse sentido, as grandes novidades trazidas pelo RGPD foram: o fortalecimento dos direitos dos indivíduos sobre seus dados; a obrigação de harmonização das normas sobre o tema para os reguladores europeus; e maior responsabilidade pra as empresas em relação aos dados pessoais que coletam, com sanções mais duras para aquelas que não agirem em conformidade com as novas regras (IRAMINA apud CONSUMRS INTERNATIONAL, 2020, p. 94).

Dentre os fundamentos jurídicos que deram ensejo ao novo regulamento europeu, é relevante destacar a harmonização das leis de proteção de dados existentes em cada país do continente (LEE, 2018, p. 68), tendo em vista que, como já mencionado, a Diretiva de Proteção de Dados não poderia ser implementada diretamente, devendo ser recepcionada por cada país, de acordo com suas leis nacionais para, assim, ser aplicada ao caso concreto (LEE. 2018, p. 34).

Caetano (2020, p. 9) ensina que o RGPD, diferente da DPD, possui um caráter transnacional, fundamentado da globalização do acesso aos dados. A inovação do seu texto está no chamado Escopo Extraterritorial (Extraterritorial Scope), isso quer dizer que, “seu objetivo principal é transpor as barreiras físicas e alcançar também

[7] Artigo 8º Protecção de dados pessoais
1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito.
2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação.
3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

toda e qualquer conduta de empresas e organizações que manipulam dados pessoais de cidadãos europeus, seja em parte ou em totalidade, fora do território comum do bloco" (VERMEULEN; LIEVENS; LIEVENS, 2017, p. 78). Assim, sua aplicação é estendida as pessoas jurídicas cujas atividades estejam respaldadas na utilização de dados pessoais na União Europeia[8].

De acordo com o Tratado sobre o Funcionamento da União Europeia TFUE, documento que organiza o funcionamento da União e determina os domínios, a delimitação e as regras de exercício das suas competências, o fundamento para a necessidade de criação de um regulamento geral se encontra no plasmado n.º 2, do art. 16.º (MELO, 2019, p. 24):

> "(…) estabelecem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União e à livre circulação desses atos. (...)".

Melo (2019, p. 25) explica que o RGPD prevê um conjunto único de regras consistentes de proteção de dados em toda a UE, estabelecendo um ambiente de segurança jurídica do qual os operadores econômicos e os titulares dos dados podem beneficiar, o que contribuiu para a modernização da legislação da UE, tornando-a adequada para proteger os direitos fundamentais no contexto dos desafios económicos e sociais da era digital. Verifica-se, portanto, a harmonização da legislação, coerência do tratamento de dados pessoas e segurança jurídica.

---

[8] Artigo 3.º Âmbito de aplicação territorial

1. O presente regulamento aplica-se ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União.

2. O presente regulamento aplica-se ao tratamento de dados pessoais de titulares que se encontrem no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com:

a) A oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento;
b) O controlo do seu comportamento, desde que esse comportamento tenha lugar na União.

3. O presente regulamento aplica-se ao tratamento de dados pessoais por um responsável pelo tratamento estabelecido não na União, mas num lugar em que se aplique o direito de um Estado-Membro por força do direito internacional público.

Dentre as inúmeras regras centrais trazidas pelo Regulamento Geral de Proteção de Dados – RGPD, cita-se o consentimento, também inserido no texto da LGPD, como se verá mais adiante. Segundo Iramina (2020, p. 94) a exigência de consentimento por parte do titular, deve ser realizada por meio de uma ação clara e afirmativa do indivíduo e que deve ser fornecido para cada operação de processamento ou uso de dados pessoais. As empresas devem, assim, manter um registro de quando e como o indivíduo deu o seu consentimento.

O aspecto novo é que se especificam duas formas de expressar o consentimento: mediante declaração ou mediante uma clara ação afirmativa. Deste modo, não cabe mais o denominado consentimento tácito (o silêncio, as alternativas já marcadas ou a inação). Logo, fica claro que o silêncio ou a inação não podem considerar-se como uma declaração de consentimento, pois este tem que ser um ato afirmativo claro e para finalidades específicas. O RGPD sinaliza em prol dos atos comissivos e não dos omissivos (LIMBERGER, 2020, p. 07).

Frise-se que o consentimento já tinha previsão na diretiva europeia ora revogada, que o adjetivou na tentativa de operacionalizá-lo. A sua qualificação como devendo ser livre, informado, inequívoco, explícito e/ou específico é uma das características marcantes do progresso geracional das leis de proteção de dados pessoais, na medida em que procura resolver a problemática em torno de um controle ilusório ou pouco efetivo das informações pessoais por parte do seu titular (BIONI, 2019, p. 161). Isso demonstra a sua imprescindibilidade no contexto da proteção de dados.

Ao retomar para o arcabouço normativo do RGPD, novamente no que que se refere ao consentimento, importante trazer à baila o disposto no art. 7º que traz as condições aplicáveis ao consentimento: 1. Quando o tratamento for realizado com base no consentimento, o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais; 2. Se o consentimento do titular dos dados for dado no contexto de uma declaração escrita que diga também respeito a outros assuntos, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente desses outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples. Não é vinculativa qualquer parte dessa declaração que constitua violação do presente regulamento; 3. O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento. A retirada do consentimento não compromete a

licitude do tratamento efetuado com base no consentimento previamente dado. Antes de dar o seu consentimento, o titular dos dados é informado desse facto. O consentimento deve ser tão fácil de retirar quanto de dar; 4. Ao avaliar se o consentimento é dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato.

Logo, segundo Melo (2019, p. 40) o pedido de consentimento deve constar de uma declaração escrita e deve distinguir-se de outras matérias que também constem dessa declaração; deve ser inteligível, de fácil acesso e ser dotado de linguagem clara e simples. Assim, um consentimento dado de forma oral ou até mediante um consentimento tácito ou outro não oferece estas garantias, porquanto não permite fazer prova de ter sido obtido de forma livre, específica, informada, explícita e através de ato inequívoco.

Para ela, é necessário que o titular previamente conheça as condições do tratamento dos seus dados, mediante a prestação de um conjunto de informações prévias relativas ao tratamento, daí o titular gozar do direito à informação (de acordo com o considerando 42, o consentimento só será informado se o titular dos dados conhecer no mínimo a identidade do responsável pelo tratamento e as finalidades a que o tratamento se destina) (MELO, 2019, p. 40).

Ademais, o titular dos dados deve ter a possibilidade de retirar o seu consentimento a qualquer momento, que deve ser tão fácil como o ato de consentir. Esta disposição obriga a que as organizações permitam a retirada do consentimento pela mesma forma em que foi concedido. No que concerne à retirada do consentimento, importa salientar que não fica comprometida a licitude do tratamento efetuado com base na sua prévia prestação (MELO, 2019, p. 41).

Iramina (2020, p. 96) adverte que o RGPD incorpora também uma abordagem de avaliação de riscos, no art. 24, que obriga as organizações não apenas a avaliar os riscos de dano aos indivíduos, mas também os benefícios que estão associados a usos específicos de informações pessoais e que possibilitam ações de mitigação de riscos que são elaboradas de acordo com a avaliação de risco/benefício feita pela empresa. De acordo com o regulamento, as organizações têm flexibilidade para determinar suas próprias metodologias de avaliação de riscos e ações de mitigação, de modo a facilitar tanto a melhor proteção da privacidade quanto o uso mais efetivo

de dados pessoais (CIPL, 2019a). Quando os dados são considerados de risco, o RGPD, no art. 35, demanda, ainda, que as empresas façam uma avaliação de impacto da proteção de dados (Data Protection Impact Assessment).

Além da figura do consentimento, Iramina (2020, p. 97) menciona que o RGPD prevê a inserção das autoridades de proteção de dados (DPAs) – ao menos uma para cada Estado Membro da UE - que são responsáveis por supervisionar, por meio de poderes investigativos e corretivos, a aplicação da lei de proteção de dados. Além de fornecer pareceres sobre questões envolvendo proteção de dados, essas autoridades que analisam as denúncias a respeito de violações ao regulamento. Até por isso, a norma dá poderes para que as autoridades de proteção de dados reguladoras imponham multas de até 20 milhões de euros ou 4% do faturamento global para algumas violações do regulamento.

Destaca-se que as DPAs trabalham em conjunto com o Comitê Europeu de Proteção de Dados (ou the European Data Protection Board - the Board) para assegurar a aplicação das normas de proteção de dados existentes no continente, bem como no âmbito transnacional. Isso garante uma maior efetivação das normas, já que ambos órgãos trabalham em cooperação.

Para uma maior compreensão, as DPAs podem ser comparadas com a Autoridade Nacional de Proteção de Dados – ANPD brasileira, criada pela Medida Provisória (MP) nº 869, de 27 de dezembro de 2018, autarquia federal de natureza especial vinculada ao Ministério da Justiça e Segurança Pública e possui a função de fiscalizar e divulgar como os dados pessoais que circulam e são utilizados pelas empresas devem ser tratados, em verdade, ela responsável por fiscalizar e fazer cumprir as disposições previstas na LGPD.

4 A APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS NAS BIG TECHS

O presente capítulo se reservou a traçar os principais tópicos da Lei Geral de Proteção de Dados – LGPD e trazer uma reflexão acerca de possíveis reflexões que servirão para compreender como o capitalismo de vigilância é praticado no setor empresarial no Brasil, em especial quando se trata das *big techs*. Para tanto, foi preciso levantar o debate sobre o modo como a vigilância operada pelas empresas pode levar à violação dos direitos fundamentais à privacidade e proteção de dados, bem como as soluções jurídicas para que haja um equilíbrio entre a proteção dos dados pessoais e a comercialização de dados de forma lícita.

4.1 A LEI N. 13.709/2018 – LEI GERAL DE PROTEÇÃO DE DADOS - LGPD

A Lei Geral de Proteção de Dados nasceu da necessidade social de se estabelecer regras para lidar com esses novos desafios derivados da coleta de dados (FREDES; BORGES, 2021, p. 186). Ela foi criada a partir do Projeto de Lei – PL número 4.060/2012 de autoria do Deputado Federal Milton Monti. Na justificativa do Projeto de Lei, consta a necessidade de "dar ordenamento jurídico e institucional ao tratamento de dados pessoais, bem como a proteção dos direitos individuais das pessoas, de acordo com a CRFB/1988" (BRASIL, 2012).

A PL foi aprovada pelo Senado em 2018 e gerou a Lei no 13.709 de 14 de agosto de 2018, sancionada pelo então Presidente Michel Temer e publicada. Entretanto, entrou em vigor apenas em setembro de 2020, com ressalva ao período de *vacatio legis* previsto em seu art. 65[9].

Inspirada no Regulamento Geral de Proteção de Dados da União Europeia (*General Data Protection Regulation*) – RGPD, a LGPD "dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de

[9] Art. 65. Esta Lei entra em vigor: (Redação dada pela Lei nº 13.853, de 2019)
I - dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e (Incluído pela Lei nº 13.853, de 2019)
I-A – dia 1º de agosto de 2021, quanto aos arts. 52, 53 e 54; (Incluído pela Lei nº 14.010, de 2020)
II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos. (Incluído pela Lei nº 13.853, de 2019)

liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (BRASIL, 2018).

Assim como no regulamento europeu, a LGPD se preocupa com o empoderamento dos titulares de dados por meio de controle e escolha significativos em relação às suas informações pessoais. Por exemplo, os titulares de dados devem ser devidamente informados sobre o processamento dos seus dados pessoais e essa informação deve ser clara, adequada, facilmente acessível e transparente (IRAMINA, 2020, p. 99).

A LGPD estabelece diretrizes e obrigações para empresas, organizações e órgãos governamentais que lidam com dados pessoais. Trata-se de um grande progresso na tutela do atual direito fundamental à proteção de dados, que passou a constar nesse rol (art. 5, LXXIX) a partir da promulgação da Emenda Constitucional n. 115/2022, consubstanciado na era da tecnologia da informação.

Assim, além de positivar questões concernentes ao direito à proteção de dados, a lei traz em seu texto alguns conceitos que merecem destaque. Inicialmente, descreve dado pessoal como sendo a informação relacionada a pessoa natural identificada ou identificável. Já por dado pessoal sensível aquele sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, quando vinculado a uma pessoa natural. Por fim, dado anonimizado como aquele relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento (BRASIL, 2018).

Enquadram-se em uma categoria especial os dados pessoais considerados sensíveis (Artigo 5º, Inciso II, da LGPD), à medida que podem sujeitar o titular dos dados a práticas discriminatórias. Os dados sensíveis são aqueles, por exemplo, sobre origem racial, convicção religiosa, opinião política, filiação a sindicato, saúde, vida sexual, dado genético, dado biométrico, entre outros. O tratamento desses dados deverá observar bases legais mais restritivas em comparação com os dados pessoais, o cuidado do legislador diz respeito aos riscos e às vulnerabilidades mais potencialmente mais gravosas aos direitos fundamentais (VAINZOF, 2019, p. 92).

O dado, então, é uma informação deixada por uma pessoa natural quando do acesso a um determinado sítio eletrônico, objeto de tratamento e organização pelas empresas, e necessário para movimentar o novo mercado digital. Já a anonimização é a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento,

por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo (BRASIL, 2019).

Importante destacar que a anonimização não pode ser confundida com a ideia de anonimato. Essa é uma das razões para existir uma “escuridão” para o legislador definir a tutela jurídica de proteção direito de dados e privacidade, porquanto ainda pairam dúvidas quanto aos reflexos da anonimização e a possibilidade de reversão. O critério da anonimização não define apenas como pessoais os dados que, imediatamente, identifiquem uma pessoa natural (viés do critério reducionista), como poderia ser informações como o nome, número do CPF, imagem etc., mas abarcou também os dados que tornam a pessoa identificável de forma não imediata ou direta”. (COTS e OLIVEIRA, 2019, p. 71).

Em síntese, a anonimização é o processo técnico que nada mais representa do que a dissociação entre determinado dado pessoal e o seu respectivo titular. Para seu implemento, inúmeros procedimentos específicos podem ser utilizados, quase sempre a partir da eliminação de determinados elementos identificadores que constam de uma base de dados, por meio de supressão do dado, generalização, randomização ou pseudonimização. (MARTINS; FALEIROS; JÚNIOR, 2019, p. 61).

Frise-se que os dados pseudoanonimizados não estão excluídos da incidência da lei. Segundo o artigo 12 da LGPD, estão excluídos para fins de incidência da lei aqueles dados anonimizados nos quais o processo de anonimização não permitir reversão. Já os dados pseudoanonimizados são aqueles cuja reversão é possível através de técnica que esteja em posse do controlador (COTS; OLIVEIRA, 2019, p. 120).

O crescimento exponencial do meio digital é uma realidade que não pode ser ignorada. Entretanto, na medida em que esse avanço é visto como positivo, uma vez que promove o acesso à informação, por outro lado, também impulsiona um dever estatal de proteção, especialmente de educação quanto aos perigos que residem no ciberespaço, tendo em vista a vulnerabilidade dos usuários. Á exemplo, cita-se os numerosos casos de vazamentos de dados, e o próprio capitalismo de vigilância. A LGPD, portanto, significa um forte progresso na tutela do direito à proteção de dados.

No avanço da análise dos dispositivos da lei, é importante trazer à baila alguns os objetivos que norteiam a LGPD, quais sejam, a proteção da liberdade, privacidade

e o livre desenvolvimento da personalidade da pessoa natural[10]. Também cabe mencionar os fundamentos que levaram o legislador a criar tais normas, estes com previsão no art. 2º[11] da LGPD. Dentre eles, destacam-se: o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor.

A autodeterminação informativa é considerada como direito fundamental, uma vez que compreende uma forma de garantir ao indivíduo o controla e proteção de seus próprios dados pessoais. A informação de cada indivíduo, aqui denominada como dado, aporta consigo um valor social, sendo o construto que é eixo estruturante da atual forma de organização social, entendido como elemento nuclear para o avanço da economia e fator determinante para a produção de riquezas, como já foram a terra, máquinas a vapor e eletricidade (BIONI, 2019, p. 4). Por isso a imprescindibilidade tão acentuada de uma maior tutela do Estado.

Ademais, a LGPD prevê alguns princípios considerados como fundamentos básicos que orientam o tratamento de dados pessoais pelas organizações e garantem a proteção dos direitos dos titulares desses dados, quais sejam, boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas. Eles têm como finalidade propiciar a privacidade, a segurança e a transparência no tratamento das informações pessoais.

De início, tem-se que a boa-fé objetiva é o pressuposto basilar no tratamento de dados pessoais. Ela é considerada como cláusula geral da LGPD e estabelece que o procedimento em epígrafe deve ser executado respeito e transparência aos direitos dos usuários. Nesse sentido, as organizações que recolhem e tratam dados pessoais

---

[10] Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

[11] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
I - o respeito à privacidade;
II - a autodeterminação informativa;
III - a liberdade de expressão, de informação, de comunicação e de opinião;
IV - a inviolabilidade da intimidade, da honra e da imagem;
V - o desenvolvimento econômico e tecnológico e a inovação;
VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

devem se portar de modo claro e objetivo em relação aos titulares, garantindo que estes tenham ciência da finalidade do tratamento e de que maneira suas informações serão utilizadas.

Boa-fé é um pensar refletido, é o pensar no outro, no mais fraco, no parceiro contratual, nas suas expectativas legítimas, é lealdade, é transparência, é informação, é cooperação, é cuidado, é visualização e respeito pelo outro. Boa fé é cooperação e respeito, é conduta esperada e leal, tutelada em todas as relações sociais. A proteção da boa-fé e da confiança despertada formam, a base do tráfico jurídico, a base de todas as vinculações jurídicas, o princípio máximo das relações contratuais (MARQUES, 2002, p. 53)

Em outras palavras, é necessário que as empresas procedam a sistemática de forma ética, com o fito de prevenir qualquer tipo de ocultação ou manipulação. Frise-se que a hermenêutica irá auxiliar na percepção da intenção das grandes empresas que recebem os dados, sendo que estas não podem se amparar no fundamento de que o consentimento em aceitar termos de uso e *cookies* que precedem a coleta, autorizam o uso indiscriminado das informações.

O princípio da finalidade também está dentre os essenciais para a proteção de dados, pois constitui um verdadeiro limitador associado diretamente ao propósito da captação de informações comunicada ao titular. Dele, decorrem outros quatro princípios previstos no art. 6º[12] da LGPD, a saber: adequação, necessidade, transparência e qualidade dos dados.

[12] 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; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; 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.

Em verdade, o princípio da finalidade está ligado à vedação do tratamento posterior dos dados de forma antagônica aos propósitos originais. Logo, diante desse preceito, ficam as empresas obrigadas a informar aos usuários o motivo pelo qual seus dados estão sendo coletados e como serão manuseados. Ademais, o tratamento só será considerado legal quando respeitar a uma base legal específica, isto é, a legislação e o consentimento do titular, este último, desde que comunicado previamente. Caso seja necessário utilizar o dado de forma diversa daquela originalmente pretendida, deverá informar ao usuário e obter uma nova aquiescência.

Importante destacar que a lei prevê, em seu art. 8º, § 5º[13] que o consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação (BRASIL, 2019). O consentimento é uma manifestação livre e inequívoca do usuário. Ele é realizado, em regra, através da aceitação da política de privacidade ou *cookies*, no qual o usuário autoriza a coleta, o uso, o armazenamento e o compartilhamento de suas informações pessoais por parte do agente tratador de dados, à exemplo, as *big techs*.

Ele deve ser alcançado de maneira individual para cada finalidade de tratamento. Assim, as empresas devem pugnar pela anuência do usuário de forma específica para cada atividade que abranja o uso de dados. Ademais, é preciso ter clareza na disposição do “termo de consentimento”, sendo vedado o uso de conteúdos genéricos nos contratos. Outro ponto importante é que o usuário pode revogar a aquiescência a qualquer tempo e essa revogação deve ser realizada através de um trâmite simples, sem burocracias excessivas.

---

[13] Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais. § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei. § 3º É vedado o tratamento de dados pessoais mediante vício de consentimento. § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas. § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.§ 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

Embora o exercício do direito de controle do indivíduo sobre as suas informações consista em uma dimensão importante da disciplina de proteção de dados pessoais, a sua forma de implementação é bastante complexa, num contexto caracterizado pela sociedade de massas e pela constante inovação tecnológica, em que nem sempre é possível ao indivíduo dimensionar as consequências futuras de uma disposição em relação aos seus dados. Dessa forma, para que o tratamento de dados pessoais baseado no consentimento seja legítimo, é preciso que o controlador se certifique de que o consentimento foi dado de forma livre e informada, resguardando não apenas a liberdade de escolha meramente formal do indivíduo, mas efetivamente a sua liberdade material (MENDES, 2014, p. 65).

O princípio da adequação, por seu turno, está previsto no art. 6º, inciso II, da LGPD e estabelece que o tratamento de dados pessoais deve ser limitado ao mínimo necessário para o desempenho dos propósitos que foram informados ao titular dos dados no momento da coleta. Assim, as empresas responsáveis devem assegurar que apenas as informações necessárias para cumprir os objetivos dispostos nos termos de uso sejam manuseados, à exemplo, pode-se citar a captação de uma predileção do usuário do *Twitter*, ser utilizada como meio de publicidade no *Instagram*, ou vice-versa.

Corolário à adequação, a lei também dispôs acerca do princípio da necessidade. Trata-se da limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados (Brasil, 2019). A captação, tratamento e uso de informações pessoais devem estar associadas à intenção pretendida (aqui recai também o princípio da boa-fé), assegurando que unicamente sejam utilizados dados estritamente necessários. Trata-se uma “norma de repressão” com o intuito de reduzir o uso inadequado de dados pessoais, resguardando a privacidade e os direitos fundamentais dos titulares.

Em verdade, últimos dois princípios aqui colacionados então interligados. Nesse sentido, Miragem (2019, p. 09-10) ensina que todo e qualquer atividade de tratamento de dados deverá se dar sobre dados “adequados” e “necessários” (art. 6º, II e III), sendo os primeiros definidos como a compatibilidade do tratamento com as finalidades informadas pelo controlador ao titular e o segundo como a limitação do tratamento ao mínimo necessário à finalidade para os quais estão sendo tratados.

A adequação e necessidade figuram-se no termo “minimização de dados”, que significa que as informações pessoais devem ser coletadas apenas em quantidade relevante e mínima para alcançar o desígnio pretendido, pactuado anteriormente com o usuário. Esse é uma das bases da legislação de proteção de dados da União Europeia, o Regulamento Geral de Proteção de Dados (*General Data Protection Regulation*) – GDPR, prevista em seu art. 5º, parágrafo 1(c)[14].

O livre acesso assegura aos titulares a consulta, a qualquer tempo, sobre como seus dados estão sendo tratados, seja por entidades públicas ou privadas. Ele tem por objetivo de viabilizar a transparência e controle das informações pelos usuários, e decorre do direito ao acesso à informação, previsto no art. 5º inciso XXXIII[15], bem como no inciso II do § 3 do art. 37[16] da Constituição Federal de 1988. Noutro giro, a qualidade de dados determina que as bases devem ser precisas, atualizadas, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento (BRASIL, 2019). Frise-se que novamente se traz à baila a ideia de consentimento do usuário para que os dados sejam mentidos atualizados, visto que esse procedimento depende da captura de novas informações.

A transparência também está dentre o rol de princípios da LGPD. Em síntese, tem como fundamento o dever das empresas e organizações serem claras no que concerne ao objetivo do tratamento de dados, de forma a oferecer informações compreensíveis aos usuários. A transparência expressa a garantia aos titulares de informações que sejam claras, precisas e facilmente acessíveis acerca da realização do tratamento e os respectivos agentes de tratamento. Isso implica na obrigação de serem disponibilizados aos titulares, a qualquer momento, acesso livre e irrestrito aos

---

[14] Artigo 5.o Princípios relativos ao tratamento de dados pessoais Os dados pessoais são: [...] c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados

[15] 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: XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado; (Regulamento) (Vide Lei nº 12.527, de 2011)

[16] Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte: (Redação dada pela Emenda Constitucional nº 19, de 1998) § 3º A lei disciplinará as formas de participação do usuário na administração pública direta e indireta, regulando especialmente: (Redação dada pela Emenda Constitucional nº 19, de 1998) II - o acesso dos usuários a registros administrativos e a informações sobre atos de governo, observado o disposto no art. 5º, X e XXXIII; (Incluído pela Emenda Constitucional nº 19, de 1998) (Vide Lei nº 12.527, de 2011)

seus dados pessoais que estão sendo objeto de tratamento pelo controlador (FEIGELSON; SIQUEIRA; 2019, p. 37).

A segurança adverte que no tratamento de dados sejam utilizadas técnicas com o fito de proteger os dados pessoais. O objetivo é evitar que informações sejam vazadas e causem algum dano ao usuário. Trata-se de um risco *in abstrato*. Importante destacar que esse princípio é pertinente em situações em que a perda do dado é resultante de um ato involuntário, logo, atribui à organização ou empresa a responsabilidade objetiva, isto é, independe de culpa. A prevenção está diretamente interligada com a segurança, já que nele há a previsão de que o tratador de dados adote medidas para acautelar as informações para que o uso destas não gere dano de qualquer natureza ao titular.

É importante destacar que a LGPD determina regras sobre padrões de segurança da informação e medidas administrativas capazes de proteger os dados pessoais que deverão ser cumpridas pelos controladores e pelos operadores (aquele que realiza o tratamento de dados pessoais em nome do controlador). Ou seja, medidas técnicas – adotadas no âmbito da tecnologia da informação e administrativas – políticas corporativas, gestão estratégica e capacitação (BONI, 2019, p. 330).

O princípio da não-discriminação também consta no rol da LGPD. Trata-se da responsabilidade atribuída ao tratador de não manipular os dados com fim ilícito ou abusivo. Cita-se como exemplo a segmentação de grupos vulneráveis, o que inclui discriminação do algoritmo com relação à raça, etnia, orientação sexual, gênero, religião, deficiência, entre outros. É uma forma ética e moral de tratar os dados, com fundamento intrínseco na dignidade da pessoa humana.

Tem-se também a responsabilização (*accountability*) e prestação de contas. Através deles é possível concluir que as empresas e organizações devem assumir a responsabilidade, de acordo com a lei, por todos os procedimentos realizados com os dados, seja na captura, tratamento ou monetização. É imprescindível que elas façam uso de ferramentas que coloquem em prática o direito a proteção de dados, com fito de proteger os usuários de qualquer atividade ilícita que possa causar danos aos titulares.

No mesmo enfoque, a norma estabelece direitos fundamentais para os sujeitos em relação a proteção de seus dados em seu art. 18, todos diretamente relacionados com os princípios já destacados, quais sejam:

> I - confirmação da existência de tratamento;
> II - acesso aos dados;
> III - correção de dados incompletos, inexatos ou desatualizados;
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;
> VI - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
> VII - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
> VIII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> IX - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> X - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

Importante destacar que a LGPD dispõe também sobre a Autoridade Nacional de Proteção de Dados – ANPD, uma autarquia federal de natureza especial do Brasil que, atualmente, se encontra vinculada ao Ministério da Justiça e Segurança Pública. O artigo 46, § 1º[17] da LGPD prevê que a ANPD poderá padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

A ANPD foi criada pela Medida Provisória nº 869, de 27 de dezembro de 2018, posteriormente convertida na Lei nº 13.853, de 14 de agosto de 2019. Foram atribuídas a ela 24 (vinte e quatro) competências, dentre as quais destacam-se: zelar pela proteção dos dados pessoais; zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações; elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; fiscalizar e aplicar sanções em caso de tratamento de dados realizado

[17] Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

em descumprimento à legislação; promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, dentre outros.

Sua estrutura organizacional, de acordo com art. 55-C é composta por Conselho Diretor, órgão máximo de direção; Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; corregedoria; ouvidoria; procuradoria; unidades administrativas e unidades especializadas. Ademais, o Conselho Diretor da ANPD será composto de 5 (cinco) diretores, incluído o Diretor-Presidente, que serão escolhidos pelo Presidente da República e por ele nomeados, após aprovação pelo Senado Federal, nos termos da alínea ‘f’ do inciso III do art. 52 da Constituição Federal, e ocuparão cargo em comissão do Grupo-Direção e Assessoramento Superiores - DAS, no mínimo, de nível 5 (BRASIL, 2020).

Ocorre que a ANPD necessita de uma estruturação atualizada e moderna, tendo em vista que função precípua, para além de regular interesses relacionados à prestação de serviços públicos ou da atuação econômica, é a de servir, em síntese, como uma guardiã de direitos fundamentais, protegendo as projeções do humano frente às investidas de entidades que se coloquem como novas mercadoras, ou, ainda, de governantes seduzidos pelo poder informacional do qual são dotados Estados supervigilantes e tecnocráticos (SARLET; RODRIGUEZ; 2022, p. 29).

Sabe-se que ao tempo em que o ciberespaço oferece uma gama de benefícios, especialmente relacionados ao direito à informação, também traz inúmeras problemáticas que carecem de legislação específica. A partir do estudo dos principais pontos da LGPD, foi possível verificar que as elucidações nela contidas, bem como normas e princípios não são, por si só, suficientes para que a proteção dos dados seja eficaz. Nesse contexto, a ANPD possui um papel importante na aplicação das diretrizes estabelecidas na Lei Geral, todavia, também carece de lapidação, especialmente no tocante ao aprimoramento da sua estrutura organizacional e capacitação dos servidores. As questões que envolvem proteção de dados ainda não muito complexas e precisam ser analisadas por profissionais capacitados na área, com o objetivo de ter uma maior eficácia na aplicação da legislação vigente.

4.2 A POLÍTICA DE COOKIES E A VULNERABILIDADE DO USUÁRIO FRENTE A IDEIA DE CONSENTIMENTO

Nos últimos anos, houve um crescimento exponencial do ambiente virtual, aqui chamado de Ciberespaço (LEVY, 1999), resultado da revolução tecno-científica informacional, na medida em que as Tecnologias da Informação e da Comunicação (TICs) transpuseram a vida social, bem como através da ascensão das *Big Techs*.

Em consequência disso, surgiram diversos imbróglios decorrentes de atividades a ela inerentes, que, na teoria estão de acordo com a legislação pátria, todavia, na prática, são responsáveis por violar direitos fundamentais. O que acontece é que usuário da rede pressupõe que possui o controle das informações ora compartilhadas com fundamento em uma “falsa” ideia de consentimento, no entanto, isso não é real.

Um exemplo claro disso é a política de cookies, o famoso “Aceito; Rejeito Todos os Cookies” presentes nas inúmeras plataformas da rede. Eles foram inventados em 1994 por Louis Montulli, engenheiro de software da Netscape, empresa conhecida pelo navegador web de mesmo nome, o mais usado durante a década de 1990 (NORMAN, 2022). Os cookies são pequenos arquivos de texto depositados pelo site provedor de conteúdo, ou servidor, no computador do usuário, ou cliente, para os fins de “recordar” o status da conexão e algumas informações pessoais do internauta (CAHN, et. al., 2016, p. 891).

De acordo com França (2015, p. 96) um cookie pode ser definido como um pequeno arquivo de texto armazenado pelo navegador (web browser), funcionando como uma “carteira de identidade” do usuário, permitindo a memorização de dados e o reconhecimento de hábitos de navegação que podem ser transformados em informações importantes tanto para o aprimoramento dos sites quanto para a oferta de publicidade personalizada, constituindo-se num polêmico mecanismo de vigilância. Eles não são ilegais, todavia, o uso de forma desenfreada e desregulada, acarreta prejuízos de tempo, dinheiro e invasão de privacidade para o usuário (PRATES, 2014, p. 42).

Os cookies são arquivos que são depositados no computador do indivíduo pelo site acessado e que possibilitam a identificação deste usuário com o intuito de facilitar a funcionalidade da página e o monitoramento da navegação, de forma que podem ser oriundos das páginas visitadas, de outras entidades (cookies de terceiros),

apagáveis (cookies de sessão) ou persistentes (cookies permanentes) (CASTELLUCCIA, 2012, p. 23-24).

Eles podem ser classificados quanto ao tipo, sendo possível distinguir cookies originais e cookies de terceiros. Os cookies originais (também designados “primários”) são definidos pelo domínio do site listado na barra de endereços, são usados para reconhecer o utilizador quando visita o website; os cookies de terceiros vêm de outras fontes de domínio que têm itens incorporados na página, como anúncios, imagens, videoclips, e pretendem reconhecer o computador do utilizador quando ele visita o website ou outros websites (ALDEIAS, 2012, p. 04).

Podem permanecer no disco do computador por diferentes períodos de tempo. Alguns são designados cookies de sessão, pois existem somente quando o website é aberto. Estes são apagados automaticamente quando o utilizador fecha o browser. Outros são cookies permanentes, pois perduram mesmo com o browser fechado. Estes podem ser usados por websites para reconhecer o computador do utilizador quando mais tarde ele voltar a abrir o seu browser e aceder à Internet outra vez (ALDEIAS, 2012, p. 04).

Castelluccia (2012, p. 23-4) alerta que existem alguns tipos cuja gestão é complexa, são os chamados supercookies e os evercookies. Os supercookies funcionam graças a elementos adicionais dos navegadores (plug-ins) e conseguem gerenciar os dados dos usuários de modo a contornar o controle humano sobre o que é ou não deletado. Já os evercookies são capazes de manipular técnicas de armazenamento das aplicações de navegação (como o armazenamento temporário de informações – cache) para permanecerem no computador do usuário, mesmo após serem deletados.

Ao acessar um endereço eletrônico e aceitar a política de cookies, o usuário, na teoria, estará consentindo com seus termos. Isso faz com que haja exposição dos dados, que são compartilhados e até mesmo usados como matéria-prima para a indústria do capitalismo de vigilância. Assim, a partir da adesão aos termos inseridos nos cookies, os dados são coletados sem que o indivíduo que navega, em regra, tenha conhecimento de como serão utilizados.

Oliveira e Silva (2018, p. 313) ensinam que os dados pessoais adquiriram status de ativos intangíveis, tornando-se estratégicos para os negócios no setor. Empresas como Google, Amazon, Uber e Netflix possuem os dados de seus clientes como o principal ativo de sua atividade empresarial.

O tratamento de dados possui posição de destaque quando da oferta de produtos e serviços por empresas de tecnologia – as quais, por vezes, não exigem uma remuneração direta dos usuários, mas o preenchimento de cadastro, a criação de perfil e/ou o acesso aos contatos e mensagens trocadas – revela a importância fundamental dos dados na criação, desenvolvimento e manutenção do próprio modelo de negócio (TEPEDINO; TEFFÉ, 2020, p. 208).

Frise-se que apesar do nome sugestivo, a proteção de dados não se volta exclusivamente aos dados em si. O seu enfoque protetivo está no titular desses dados: quem arcará com os riscos e com as eventuais consequências prejudiciais do uso de seus dados pessoais. Nesse sentido, o papel regulatório é mais amplo: disciplinar a informação gerada a partir do processamento e do tratamento dos dados pessoais, em um devido contexto (MENDES e FONSECA, 2020, p. 517).

Por conseguinte, apesar de o dado em si permanecer importante ponto de referência regulatória para a disciplina da proteção de dados pessoais, é preciso observar essa cadeia mais ampla e pensar na regulação global dos seus usos, que vão muito além do processo de coleta inicial: as informações geradas a partir de seu processamento; as decisões tomadas a partir dessas informações; e, sobretudo, os efeitos adversos oriundos dessas decisões, porque capazes de afetar a vida e liberdade dos indivíduos envolvidos (ALBERS, 2014, p. 222-224).

O panorama formado a partir da ascensão do capitalismo de vigilância fez com que os sujeitos passassem de meros usuários da rede, para figurar como fornecedores da matéria-prima mais valiosa do ciberespaço: os dados pessoais. É a partir desse cenário que se observa a hipervulnerabilidade do indivíduo, uma vez que além de ter suas informações coletadas de forma ambígua, ainda são vítimas do novo modelo econômico baseado na publicidade predatória que analisa o perfil comportamental dos usuários para definir comportamentos e predileções com o fito de influenciar na tomada de decisão.

Diante desse novo contexto alicerçado pelo avanço da tecnologia, nas últimas décadas, a privacidade vem sendo gradualmente compreendida como direito de manter controle sobre as próprias informações, passando a fazer referência à possibilidade de a pessoa natural conhecer, controlar, endereçar e, até mesmo, interromper o fluxo das informações a ela relacionadas. Abriu-se, assim, espaço para a chamada autodeterminação informativa, que representa a faculdade de o particular

controlar a obtenção, a titularidade, o tratamento e a transmissão de dados relativos a ele (TEPEDINO; TEFFÉ, 2020, p. 206).

Tornou-se comum o procedimento de (i) informar o titular dos dados pessoais acerca de quais dados estão sendo coletados e como eles serão usados (notice); em seguida, (ii) permitir com que ele detenha o poder de decidir se aceita, ou não, os referidos usos de seus dados pessoais (consent) (SOLOVE, 2013, p. 1883).

Ocorre que importantes evidências empíricas trazidas pelas ciências comportamentais têm demonstrado que tais pressupostos nem sempre são adequados, especialmente em face de limitações cognitivas, como vieses e heurísticas, que podem dificultar a avaliação dos elementos necessários "para racionalizar um processo de tomada de decisão genuíno a respeito do fluxo de seus dados pessoais" (MENDES E FONSECA apud BIONI, 2020, p. 515).

Diante desse contexto, surge a autodeterminação informativa, prevista no art. 2º, inciso II, da LGPD, como o direito que todo sujeito possui de controlar e proteger seus dados pessoais. É ela que fundamenta a necessidade de consentimento do titular no momento da coleta e tratamento das informações.

Apesar da autodeterminação informativa ser um dos pilares da LGPD, há um problema que necessita ser solucionado ao aplicar a lei: o fato de que a tecnologia é revestida por manto de facilidade aliada com a falta de informação. Para uma maior compreensão, necessário ter em mente que, ao acessar a internet, o usuário que não possui um nível de conhecimento técnico avançado, é levado manifestar concordância com as regras de coleta e tratamento de dados ali dispostas, pois, na maioria das vezes, sequer lê o que elas dispõem por serem extensas e de difícil compreensão. A partir disso, suas informações poderão ser utilizadas de forma indiscriminada, tendo em vista houve "consentimento" para tanto. De acordo com Mendes e Fonseca (2020, p. 515):

> Apesar da grande relevância dada à apresentação de informações pela entidade responsável pelo tratamento de dados, estudos têm indicado que, ao tomar decisões sobre sua privacidade e sobre seus dados, os indivíduos muitas vezes sequer leem regularmente as "Políticas de Privacidade" ou "Informações sobre o Uso de Dados" que lhe são apresentadas (MILNE; CULNAN, 2004), o que pode tornar a medida inócua. Mais do que isso, as informações disponibilizadas costumam ser de difícil compreensão, haja vista a complexidade e sofisticação do tratamento de dados na espécie, envolvendo vários conceitos técnicos e jurídicos ou até mesmo o tamanho das letras e a extensão do texto. Em verdade, o próprio excesso de informações pode ser prejudicial, sobrecarregando a cognição do titular dos dados acerca dos efeitos atinentes às questões apresentadas (MACEDO

> JUNIOR, 1999, p. 247). Além disso, até mesmo a maneira com que essas regras e essas escolhas são disponibilizadas (framed) pode influenciar sensivelmente o processo decisório de se consentir ou não (ACQUISITI, 2009, p. 83).

O consentimento representa instrumento de manifestação individual no campo dos direitos da personalidade e tem o papel de legitimar que terceiros utilizem, em alguma medida, os dados de seu titular. Ele compreende a liberdade de escolha, sendo meio para a construção e delimitação da esfera privada. Associa-se, portanto, à autodeterminação existencial e informacional do ser humano, mostrando-se imprescindível para a proteção do indivíduo e a circulação de informações (TEPEDINO; TEFFÉ, 2020, p. 209).

Os usuários acessam as plataformas e consentem com a política de cookies para obter as vantagens oferecidas, em consequência, têm seus dados coletados e tratados. A partir disso, há a classificação das informações e utilização com o objetivo de personalizar a publicidade para determinados grupos e assim, induzi-los a adquirir produtos e até mesmo manipular a tomada de decisão. Em regra, as informações são capturadas e disponibilizadas para outras empresas que pretendem fazer a publicidade predatória. Nesse contexto, Oliveira e Silva (2018, p. 313) ensinam que:

> Nesta roda viva tecnológica dos dados pessoais, tecnologias cada vez mais invasivas são utilizadas para extrair e analisar padrões de comportamentos online e estas informações passam a constituir a base de diversas atividades empresariais. “Não existe almoço grátis” é um ditado bem pertinente quando o assunto é coleta e utilização de dados pessoais. As empresas do setor tecnológico se especializam cada vez mais para fornecer produtos aparentemente gratuitos ao usuário, cujo “preço” embutido é o da coleta, refinamento e até venda de seus dados estrategicamente.

Esse modelo de publicidade, apesar de ser considerado “legal”, com fundamento na ideia de consentimento, pode causar danos imensuráveis ao usuário, uma vez que estar-se-á diante de uma falsa sensação de controle. Isso se dá pelo fato de que se o titular não concorda com a política de cookies de um determinado website, acaba tendo o direito de acessar as funcionalidades negado. Logo, impõe a concordância dos termos, sendo quase impossível mensurar os reflexos negativos dessa simples ação.

No Brasil, a primeira legislação que regulamentou a proteção de dados pessoais na internet foi a Lei n° 12.965/2014 conhecida como Marco Civil da Internet. Acerca dos cookies, Helena Martins (2014, p. 62) afirma que marco também garante

a privacidade dos usuários da internet, ao estabelecer que informações pessoais e registros de acesso só poderão ser vendidos se o usuário autorizar expressamente a operação comercial. Atualmente, os dados são usados por grandes empresas para obter mais receitas publicitárias, já que elas têm acesso a detalhes sobre as preferências e opções dos internautas e acabam vendendo produtos direcionados.

A Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/18) conceitua o termo “consentimento” como: a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. O consentimento, no ordenamento jurídico pátrio, está diretamente atrelado aos princípios da informação e da boa-fé objetiva, elencado no art. 6º, caput, da LGPD[18].

Por “livre” compreenda-se a liberdade do titular que não pode ser forçado a consentir com o tratamento de seus dados. Por “informada” compreenda-se a transparência da informação referente à o que especificamente o titular está consentindo a fim de que ele possa tomar sua decisão de maneira consciente. Por derradeiro, entende-se por inequívoca a manifestação por parte do titular na qual não exista nenhuma dúvida sobre a verdadeira aceitação não apenas das condições, mas, também, das repercussões decorrentes do tratamento de seus dados (TEPEDINO; TEFFÉ, 2019, p. 300).

Cabe ao tratador informar, de forma completa e clara, sobre a utilização e destino dos dados pessoais coletados. Ocorre que, diferente do Regulamento Geral de Proteção de Dados – RGPD, a LGPD não especificou os itens mínimos a serem comunicados antes do usuário consentir com o uso das informações. Toniazzo (2022, p. 72-73) extrai do disposto no capítulo III, artigos 13, 14 e 15 da RGPD o mínimo a ser informado aos titulares dos dados antes do seu consentimento:

> 1. a identidade e os contatos do responsável pelo tratamento e, se for o caso, do seu representante; 2. os contatos do encarregado da proteção de dados; 3. as finalidades do tratamento a que os dados pessoais se destinam, bem como fundamento jurídico para o tratamento; 4. se o tratamento dos dados se basear no legítimo interesse, isso deve ser informado e detalhado o legítimo interesse no caso; 5. os destinatários ou categorias de destinatários dos dados pessoais, se houver; 6. se for caso, a transferência internacional dos dados pessoais, informando se o país tem um nível adequado de proteção de dados; 7. o prazo de conservação dos dados pessoais ou, se não

[18] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
[...]

> for possível, os critérios usados para definir esse prazo; 8. a existência do direito de solicitar ao responsável pelo tratamento e no que disser respeito ao titular dos dados, ou do direito de esse se opor ao tratamento, bem como do direito à portabilidade dos dados; 9. se o tratamento dos dados se basear no legítimo interesse, a existência do direito de revogar consentimento a qualquer tempo, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado; 10. o direito de apresentar reclamação a uma autoridade de controle; 11. se a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular está obrigado a fornecer os dados pessoais e as eventuais consequências de não fornecer esses dados; 12. a existência de decisões automatizadas, incluindo a definição de perfis, as informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular de dados.

Quando se trata de relações dissonantes, em que há um desequilíbrio informacional expressivo entre os agentes, como, por exemplo, o usuário e as *Big Techs*, o consentimento, apesar de ser imprescindível, não pode ser o único instrumento de legitimação para que o titular autorize a coleta e uso dos seus dados. É necessário que ele esteja alicerçado em outros pilares, como o da segurança, boa-fé, transparência e informação.

À título de exemplo no âmbito nacional, apesar de não se tratar de um caso envolvendo uma empresa considerada como *big tech*, cita-se a Ação Civil Pública de nº 0749765-29.2020.8.07.0000 proposta pelo Ministério Público do Distrito Federal em desfavor do Serasa S.A. A 2ª Turma Cível do TJDFT manteve, por unanimidade, decisão liminar que suspende a comercialização de dados pessoais dos titulares por meio dos produtos Lista Online e Prospecção de Clientes, oferecidos pelo site Serasa S.A. Nos autos, o autor destaca que a empresa comercializava dados pessoais de brasileiros, ao ofertar os serviços citados, entre eles, dados de contato, sexo, idade, poder aquisitivo, classe social, localização, modelos de afinidade e triagem de risco - prática que, no entendimento daquele órgão vai contra os princípios da Lei Geral de Proteção de Dados Pessoais – LGPD (TJDF, 2021).

O MPDFT frisou que a LGPD dispõe sobre a necessidade de “uma manifestação específica para cada uma das finalidades para as quais o dado está sendo tratado”, por isso a comercialização, nos moldes feitos pelo Serasa, seria ilegal ou irregular, pois “fere o direito à privacidade das pessoas, bem como seus direitos à intimidade e à imagem, o que inclui o direito à proteção de seus dados pessoais” (TJDF, 2021).

No voto do agravo de instrumento interposto pelo MPDFT contra decisão que, em sede de Ação Civil Pública (processo nº 0736634-81.2020.8.07.0001[19]), indeferiu o pleito liminar voltado à suspensão da comercialização de dados pessoais dos titulares por meio dos produtos “Lista Online” e “Prospecção de Clientes”, o relator desembargador César Laboissiere Loyola argumenta que:

> Consoante se observa, quanto aos dados pessoais sensíveis a LGPD dispôs, em seu art. 11º, inciso I, que o tratamento somente é cabível com o consentimento do titular ou responsável, manifestado de forma específica e destacada, ressalvadas hipóteses excepcionais, descritas no inciso II, em que é dispensado o consentimento do titular. No caso, a controvérsia entre as partes diz respeito à comercialização de dados relacionados à pessoa natural identificada (nome, endereço, CPF, números de telefones, localização, perfil financeiro, poder aquisitivo e classe social). Portanto, à luz da LGPD, conforme o artigo 5º acima transcrito, referidos dados não constituem dados sensíveis. Não obstante, o fato de dar tratamento específico aos dados sensíveis não exclui a proteção aos demais dados pessoais, conforme se extrai da interpretação do artigo 7º da LGPD. Com efeito, não há como acolher, como sustenta a agravada, o entendimento de que seria bastante para dispensa do consentimento a constatação de que o controlador tem interesse legítimo (artigo 7º, inciso IX) ou que o compartilhamento dos dados tenha finalidade de proteção do crédito (inciso X), ante uma alegada ausência de hierarquia no rol de hipóteses do art. 7º da LGPD.
>
> [...]

[19] APELAÇÃO. AÇÃO CIVIL PÚBLICA. PRELIMINAR DE NEGATIVA DE PRESTAÇÃO JURISDICIONAL. REJEITADA. COMERCIALIZAÇÃO DE PRODUTOS E FERRAMENTAS DE TRATAMENTO DE DADOS PESSOAIS. PROTEÇÃO DOS DIREITOS DO CONSUMIDOR. INOBSERVÂNCIA DA LEGISLAÇÃO DE REGÊNCIA. 1. Apelação interposta contra sentença que, em sede de ação civil pública, julgou procedente a pretensão formulada pelo Ministério Público para condenar a requerida a se abster de comercializar dados pessoais de consumidores, por meio de duas específicas ferramentas de tratamento de dados, sob pena de imposição das medidas indutivas, coercitivas, mandamentais ou sub-rogatórias necessárias para assegurar o cumprimento de ordem judicial, conforme legislação processual civil. 2. A eventual discrepância entre as teses defendidas pelos litigantes e a interpretação conferida pelo julgador às disposições normativas que disciplinam determinada matéria posta em debate não se confunde com a negativa de prestação jurisdicional. 3. Se o que está em pauta é a comercialização de dados tratados, resta evidente que as condições do tratamento - em todas as dimensões do conceito legal - devem ser examinadas. 4. A Lei nº 13.709/2018 (LGPD) dispõe que eventual dispensa da exigência do consentimento do titular das informações processadas não desobriga os agentes de tratamento das obrigações de garantir transparência acerca de todo o processo (coleta dos metadados, da metodologia utilizada, da duração do tratamento, ou do uso compartilhado, por exemplo). A referida norma determina, ainda, que sejam respeitadas a legitima expectativa do titular das informações tratadas e os direitos e liberdades fundamentais. E somente em uma relação de efetiva transparência é possível conceber a existência de legítima expectativa. 5. Mesmo que o produto final dos serviços impugnados garanta ao contratante um apanhado de informações de natureza meramente cadastral, é inafastável a conclusão de que a segmentação e o direcionamento de mercado - prometidos pela requerida - depende de tratamento de informações outras, de natureza socioeconômica e comportamental, elementos intrinsecamente vinculados à esfera da privacidade. Assim, não havendo transparência sobre os trâmites de coleta e tratamento, é impositivo o acolhimento da pretensão autoral. 6. Recurso conhecido e desprovido. (TJ-DF 07366348120208070001 DF 0736634-81.2020.8.07.0001, Relator: SANDOVAL OLIVEIRA, Data de Julgamento: 09/02/2022, 2ª Turma Cível, Data de Publicação: Publicado no PJe : 11/02/2022 . Pág.: Sem Página Cadastrada.)

> O que se extrai do art. 7º, da LGPD é que o consentimento pelo titular é a regra maior a ser observada para o tratamento de dados pessoais, tanto é que o § 4º, daquele dispositivo, prescreve textualmente - de forma a evitar dúvidas interpretativas - a dispensa do consentimento apenas para os dados tornados manifestamente públicos pelo titular.
>
> [...]
>
> Não se verifica, frise-se, na comercialização de dados pessoais, o interesse do titular- que não pode ser presumido ante a proteção legal - ou interesse público que possa justificar a dispensa do consentimento (§ 3º, inciso X, do artigo 7º da LGPD).
>
> Sendo assim, em análise preliminar e não exauriente, como é própria das decisões de tutela de urgência, considero pertinente o entendimento de que a comercialização dos dados pessoais sem o consentimento, ainda que não caracterizados como dados sensíveis, fere a legislação específica e tem potencial para ensejar violação à privacidade, intimidade e imagem das pessoas, o que evidencia a probabilidade do direito.

Restou demonstrado a relevante ameaça de lesão quando do compartilhamento de dados sem autorização pelas empresas sem autorização, o que levou a suspensão da sua comercialização, sob pena de multa de R$5 mil, por cada venda efetuada. Logo, sucede que não é exagero afirmar que o consentimento tem figurado como instrumento regulatório central e núcleo de legitimidade prática do regime protetivo de dados. Ele é lido, ainda, como expressão da autonomia individual e do controle do titular dos dados em torno de seus direitos de personalidade (BIONI, 2019, p. 177).

É clarividente que apesar do consentimento ser importante instrumento para concretizar a proteção à livre determinação da utilização de dados pelo titular, também é o responsável por uma falsa sensação de segurança. Isto porque permite que o titular se coloque em situações desvantajosas, tendo em vista que é ele quem passa a ter o dever de defender sua própria privacidade, fazendo-o através do consentimento, mas também passando a assumir o papel de responsável em caso de resultado contrário à sua proteção (GONÇALVES, 2022, p. 31).

Outro exemplo importante de violação da livre manifestação do consentimento que cita, por analogia, o REsp n° 11348532- SP[20], em que o Superior Tribunal de

[20] CONSUMIDOR. RECURSO ESPECIAL. AÇÃO DECLARATÓRIA DE INEXIGIBILIDADE DE DÉBITO POR VAZAMENTO DE DADOS BANCÁRIOS CUMULADA COM INDENIZAÇÃO POR DANOS MORAIS E REPETIÇÃO DE INDÉBITO. GOLPE DO BOLETO. TRATAMENTO DE DADOS PESSOAIS SIGILOSOS DE MANEIRA INADEQUADA. FACILITAÇÃO DA ATIVIDADE CRIMINOSA. FATO DO SERVIÇO. DEVER DE INDENIZAR PELOS PREJUÍZOS. SÚMULA 479/STJ. RECURSO ESPECIAL PROVIDO. 1. Ação declaratória de inexigibilidade de débito por vazamento de dados bancários cumulada com indenização por danos morais e repetição de indébito, ajuizada em 13/2/2020, da qual

Justiça considerou como abusiva cláusula que obrigava cliente de cartão de crédito a fornecer dados a terceiros. De acordo com o voto do Ministro Luis Felipe Salomão é abusiva e ilegal cláusula prevista em contrato de prestação de serviços de cartão de crédito, que autoriza o banco contratante a compartilhar dados dos consumidores com outras entidades financeiras, assim como com entidades mantenedoras de cadastros positivos e negativos de consumidores, sem que seja dada opção de discordar daquele compartilhamento.

Toniazzo (2022, p. 73-74) ensina que quanto mais qualificada a informação, menores as possibilidades de erro e de celebração de vínculos dos quais os titulares venham a se arrepender posteriormente. Diz-se qualificada a informação porque ela precisa ser clara, acessível e em linguagem adequada ao público que consentirá; portanto, aquele que informa deve observar a boa-fé ao fornecer as informações ao titular; só assim criar-se-ão condições ótimas entre as partes e estará assegurada a integridade, exatidão e a liberdade do consentimento emitido, livrando-o de vícios.

---

foi extraído o presente recurso especial, interposto em 15/2/2022 e concluso ao gabinete em 19/6/2023. 2. O propósito recursal consiste em decidir se a instituição financeira responde por falha na prestação de serviços bancários, consistente no vazamento de dados que facilitou a aplicação de golpe em desfavor do consumidor. 3. Se comprovada a hipótese de vazamento de dados da instituição financeira, será dela, em regra, a responsabilidade pela reparação integral de eventuais danos. Do contrário, inexistindo elementos objetivos que comprovem esse nexo causal, não há que se falar em responsabilidade das instituições financeiras pelo vazamento de dados utilizados por estelionatários para a aplicação de golpes de engenharia social (REsp 2.015.732/SP, julgado em 20/6/2023, DJe de 26/6/2023). 4. Para sustentar o nexo causal entre a atuação dos estelionatários e o vazamento de dados pessoais pelo responsável por seu tratamento, é imprescindível perquirir, com exatidão, quais dados estavam em poder dos criminosos, a fim de examinar a origem de eventual vazamento e, consequentemente, a responsabilidade dos agentes respectivos. Os nexos de causalidade e imputação, portanto, dependem da hipótese concretamente analisada. 5. Os dados sobre operações bancárias são, em regra, de tratamento exclusivo pelas instituições financeiras. No ponto, a Lei Complementar 105/2001 estabelece que as instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados (art. 1º), constituindo dever jurídico dessas entidades não revelar informações que venham a obter em razão de sua atividade profissional, salvo em situações excepcionais. Desse modo, seu armazenamento de maneira inadequada, a possibilitar que terceiros tenham conhecimento de informações sigilosas e causem prejuízos ao consumidor, configura defeito na prestação do serviço (art. 14 do CDC e art. 44 da LGPD). 6. No particular, não há como se afastar a responsabilidade da instituição financeira pela reparação dos danos decorrentes do famigerado "golpe do boleto", uma vez que os criminosos têm conhecimento de informações e dados sigilosos a respeito das atividades bancárias do consumidor. Isto é, os estelionatários sabem que o consumidor é cliente da instituição e que encaminhou e-mail à entidade com a finalidade de quitar sua dívida, bem como possuem dados relativos ao próprio financiamento obtido (quantidade de parcelas em aberto e saldo devedor do financiamento). 7. O tratamento indevido de dados pessoais bancários configura defeito na prestação de serviço, notadamente quando tais informações são utilizadas por estelionatário para facilitar a aplicação de golpe em desfavor do consumidor. 8. Entendimento em conformidade com Tema Repetitivo 466/STJ e Súmula 479/STJ: "As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias". 9. Recurso especial conhecido e provido para reformar o acórdão recorrido e reestabelecer a sentença proferida pelo Juízo de primeiro grau.

Importante destacar que na hipótese em que o consentimento é requerido, ele será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência e de forma clara e inequívoca. Quando o consentimento for necessário, havendo mudanças em relação à finalidade para o tratamento dos dados não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo este revogar o consentimento, caso discorde das alterações (TEPEDINO; TEFFÉ, 2020, p. 209). Ademais, ele poderá ser revogado mediante declaração expressa do usuário, sendo que esse procedimento deve ser simples e gratuito.

Percebe-se então que o consentimento figurou por muito tempo como núcleo de legitimidade jurídica do regime protetivo dos dados pessoais, viabilizando vários tratamentos de dados por entidades públicas e privadas: o indivíduo foi informado das práticas? Consentiu com o tratamento de dados realizado? Caso positivo, essas práticas e esses tratamentos se tornam legítimos, por terem passado pelo crivo individual do titular (SOLOVE, 2013, p. 1880-1882 *apud* DONEDA, 2019, p. 198).

No entanto, isso por si só não é suficiente. Apesar da gama de normas que regulam a coleta e tratamento dos dados, estar-se-á diante de uma situação complexa. O consentimento é considerado como pilar da legitimação da captura e tratamento de dados, todavia, as relações oriundas da ciberespaço são abstrusas e de difícil controle. É árdua a caminhada em busca de um consentimento livre, informado, inequívoco e com uma finalidade determinada, especialmente frente facilidades trazidas pela sociedade da informação.

Toniazzo *apud* Bioni (2022, p. 79) cita estudos que demonstram que os indivíduos raramente têm plena consciência sobre os riscos e ameaças aos seus dados pessoais, os quais serão brevemente sintetizados a seguir. O primeiro estudo fomentado por Bioni denominado Mental Models, das Universidades de Standford e Carnegie Mellon, investigou os modelos mentais dos usuários a respeito do funcionamento da publicidade comportamental no ambiente on-line e concluiu que uma parcela ínfima dos usuários teria conhecimento técnico para autodeterminar os seus dados pessoais nesse cenário de coleta.

O segundo estudo empírico apresentado por Bruno Bioni, que é complementar ao primeiro, no sentido de confirmar a assimetria informacional e a vulnerabilidade dos usuários no controle dos seus dados pessoais, foi realizado pela

Universidade de Berkeley, da Califórnia208, que analisou tecnologias utilizadas como elemento neutralizador da capacidade dos usuários em controlar as suas informações pessoais (TONIAZZO *apud* BIONI, 2022, p. 80).

A terceira pesquisa é da Faculdade de Comunicação Annenberg, da Universidade da Pensilvânia, que contrapõe a conclusão das anteriores de que os consumidores estariam confortáveis e conscientes da troca de seus dados pessoais por serviços e produtos (trade-off), afirmando que a grande maioria das pessoas é conivente com a lógica da economia dos dados pessoais por estarem com ela resignadas, ou seja, elas teriam simplesmente acatado algo que é indesejável, mas, ao mesmo tempo, inevitável (TONIAZZO *apud* BIONI, 2022, p. 80).

A última pesquisa é da Universidade de Bochum (Alemanha) e analisou as notificações, chamadas de aviso de cookies, "[...]promovem, de fato, transparência acerca das práticas de tratamento de dados pessoais pelas plataformas e, em última análise, auxiliam na obtenção de um consentimento válido por parte dos usuários" (TONIAZZO *apud* BIONI, 2022, p. 80).

A terceira pesquisa traduz de forma literal a dimensão da problemática abordada na presente pesquisa: de um lado, os dados são utilizados de forma imoderada e fora dos ditames legais; do outro, as pessoas são seduzidas pela ideia de facilidade trazida pelo meio virtual, tendo como única preocupação os benefícios imediatos que ele traz, sem sequer analisar minimamente as consequências.

A necessidade de primazia da boa-fé e da autodeterminação informativa no momento em que os dados são coletados é de especial relevância para a eficácia da legalidade da conduta. O agir segundo a boa-fé objetiva concretiza as exigências de probidade, correção e comportamento leal hábeis a viabilizar um adequado tráfico negocial (MARTINS-COSTA, 2018, p. 43).

Para fomentar ainda mais as problemáticas existentes no consentimento, Mendes e Fonseca (2020, p. 513) apresentam três pontos importantes que elucidam as insuficiências do consentimento como foco regulatório: (i) as limitações cognitivas do titular dos dados pessoais para avaliar os custos e benefícios envolvidos quanto aos seus direitos de personalidade; (ii) as situações em que não há uma real liberdade de escolha do titular como, por exemplo, em circunstâncias denominadas de "*take it or leave it*"; e (iii) as modernas técnicas de tratamento e análise de dados a partir de Big Data que fazem com que a totalidade do valor e a possibilidade de uso desses

dados não sejam completamente mensuráveis no momento em que o consentimento é requerido.

Na primeira o interesse do usuário é potencializado em face dos custos e benefícios envolvidos em consentir, ou não, com os termos que lhe são apresentados. Assim, caso esteja munido de amplo conhecimento acerca do que é feito com seus dados pessoais, poderá sopesar os custos envolvidos para sua personalidade e contrapô-los em face dos benefícios trazidos, por exemplo, pela utilização de um serviço online (MENDES e FONSECA, 2020, p. 513).

Isso quer dizer que a plataforma, partindo do pressuposto das *Big Techs*, objeto de estudo da presente pesquisa, informam ao usuário quais informações estão sendo coletadas e a partir disso ele escolhe entre aceitar ou não a coleta e tratamento dos seus dados. Em teoria, estar-se-á diante do consentimento previsto na LGPD. Entretanto, evidências empíricas trazidas pelas ciências comportamentais têm demonstrado que tais pressupostos nem sempre são adequados, especialmente em face de limitações cognitivas, como vieses e heurísticas, que podem dificultar a avaliação dos elementos necessários “para racionalizar um processo de tomada de decisão genuíno a respeito do fluxo de seus dados pessoais” (Mendes e Fonseca apud Bioni, 2020, p. 515).

Essas limitações cognitivas são relativas. De um lado, existem pessoas que possuem acesso à rede, mas não dispõe da mínima noção dos riscos que ela pode trazer. Do outro, sujeitos possuem capacidade racional das consequências negativas advindas, todavia, a liquidez (BAUMAN, 2003), suplementada pelo imediatismo fazem com que assumam a exposição ao perigo em troca das contingências ofertadas no dado momento.

Isso se alia ao fato de que as informações disponibilizadas costumam ser de difícil compreensão, haja vista a complexidade e sofisticação do tratamento de dados na espécie, envolvendo vários conceitos técnicos e jurídicos ou até mesmo o tamanho das letras e a extensão do texto. Em verdade, o próprio excesso de informações pode ser prejudicial, sobrecarregando a cognição do titular dos dados acerca dos efeitos atinentes às questões apresentadas (MACEDO JÚNIOR, 1999, p. 247).

As limitações de poderes demonstram uma assimetria fundada na vulnerabilidade do usuário frente ao gigantismo das *big techs*. Os termos de uso apresentam uma gama de conteúdos que carecem de um estudo técnico para uma maior compreensão, sendo lógico que grande parte dos usuários sequer possuem

acesso ao conhecimento básico que a rede dispõe, estando longe de alcançar o que se espera da autodeterminação informativa.

Frise-se que a maioria das plataformas digitais apenas oferecem a opção de aceitar ou não os termos ali dispostos. Vários desses termos negociais se baseiam em uma lógica binária "*take it or leave it*": consentir ou não consentir, sem outras opções. Porém, ao não consentir, o custo é o de não desfrutar o serviço almejado, v.g., o uso de uma rede social ou de um aplicativo online (BALKIN, 2018, p. 3). Ou seja, o consentimento se origina de uma verdadeira imposição estabelecida por terceiro: consentir ou simplesmente não desfrutar de serviço/produto, que, muitas vezes, sob a perspectiva do indivíduo, é essencial para a sua sociabilidade ou acesso à informação na era digital (MENDES; FONSECA, 2020, p. 516).

Assim, frente as atividades cotidianas e incidência do digital em seus diferentes âmbitos, o ato de não consentir acarretaria na negação do acesso ao indivíduo dos conteúdos e serviços oferecidos em rede. Nesse cenário, emerge o questionamento sobre a dificuldade quanto a determinação do livre consentimento dos usuários, vez que, a padronização desses sistemas nos sites, influem diretamente na vontade e fazem surgir a concepção de serem necessárias as permissões de utilização de seus dados, para a inserção na sociedade (LUGATI; ALMEIDA, 2020, p. 24).

A prática da permissão de forma recorrente torna a ação habitual e automática, havendo uma falsa percepção quanto à possibilidade de escolha, influenciando o usuário a se render ao mercado informacional de forma instantânea e sem racionalização (BIONI, 2019). Um dos fatores determinantes para a massificação dessa atividade, diz respeito a utilização da internet na atualidade, em setores essenciais para que o indivíduo exerça sua cidadania, de maneira principal e mais abrangente na área consumerista.

Em frente a essas insuficiências, iniciativas normativas mais recentes, como a Lei Geral de Proteção de Dados (Lei n° 13.709/2018, doravante LGPD) e o Regulamento Geral de Proteção de Dados (RGPD), têm apresentado abordagens distintas e medidas complementares com o intuito de garantir maior efetividade e segurança ao consentimento do titular dos dados (Mendes e Fonseca, 2020, p. 509).

Inclusive, a LGPD prevê a necessidade de se elaborar os relatórios de impacto à proteção de dados quando os "processos de tratamento de dados pessoais" possam "gerar riscos às liberdades civis e aos direitos fundamentais" (art. 5°, XVII). Nesse

diapasão, o controlador (agente competente para tomar as decisões atinentes ao tratamento de dados) deverá não só descrever esses processos, como também apresentar “medidas, salvaguardas e mecanismos de mitigação” dos riscos identificados (MENDES E FONSECA, 2020, p. 523).

Ocorre que a execução dessas medidas previstas na Lei Geral de Proteção de Dados necessita do envolvimento dos tratadores de dados, em especial no que tange a transparência da utilização destes, além de delimitar parâmetros para atenuar os riscos inerentes a nova atividade econômica baseada na informação.

Além disso, é imperioso estimular a incorporação da ideia de autodeterminação informativa nos sistemas, códigos, arquiteturas e procedimentos tecnológicos: aplicar o direito fundamental à proteção de dados na concepção e na aplicação das tecnologias que permeiam os serviços e produtos disponíveis aos usuários (MENDES E FONSECA, 2020, p. 521).

Na prática, os autores supramencionados citam as PETs (Privacy Enhancing Technologies), tecnologias que fortalecem a proteção de dados pessoais e/ou simplesmente são facilitadoras da fruição desse direito ao inserir outros mecanismos de estratégias regulatórias. Aduzem também que alguns exemplos atuais merecem destaque:

> [...] criptografia de ponta a ponta” utilizada por aplicativos como o Whatsapp a fim de converter mensagens de texto, voz e vídeo em dados cifrados. Assim, apenas os participantes da comunicação (as “pontas” representadas pelo emissor e receptor ou o grupo envolvido) podem decifrá-los. Nesse sentido, a medida é benéfica à proteção de dados ao aumentar a confiança dos seus usuários e a segurança do sistema tecnológico, impedindo ou dificultando acessos indevidos (Mendes e Fonseca *apud* Abreu 2020, p. 521).

A normalização do ato de consentimento de forma automática e sem maior compreensão sobre as condições e termos impostos, faz surgir a necessidade de discutir e avaliar quais as futuras possíveis consequências das ações realizadas pelos sites. Isto porque, ao coletar, utilizar, tratar e armazenar os dados pessoais, pode ocorrer a utilização indevida destes para fins desconhecidos pelos usuários que exercem a concordância com o intuito de utilizarem as informações e serviços contidos em determinado site, porém sem se atentaram as consequências oriundas da adesão. Para isso, a essa regra, faz-se necessário a incorporação dos princípios previstos em lei, além de estratégias práticas e inovadoras para que haja uma maior proteção do usuário, utilizando a própria tecnologia a favor.

4.3 O DIREITO A AUTODETERMINAÇÃO INFORMATIVA COMO FUNDAMENTO PARA O CONSENTIMENTO

No ordenamento pátrio, nos moldes do art. 5º, inciso X da Constituição Federal, os direitos à intimidade, a vida privada, a honra e a imagem das pessoas são tuteladas como invioláveis e fundamentais, assegurando o direito à indenização pelo dano material ou moral decorrente da sua violação (BRASIL, 1988). Sendo ainda, a inviolabilidade a vida privada essa também protegida no artigo 21 do Código Civil.

A intimidade e a vida privada, são institutos titulares de certas semelhanças, porém não constituem um único significado. Como forma de elucidar as particularidades de cada um, Mendes (2012, p. 407- 408) conceitua a privacidade como um direito relacionado a preservação dos comportamentos e acontecimentos atinentes aos relacionamentos pessoais em geral que o indivíduo não deseja que se espalhem ao conhecimento público, já o direito à intimidade estaria atrelado a conversações e episódios ainda mais íntimos, individuais e particulares.

Com o advento da revolução digital e tecnológica, os referidos direitos ganharam novos ângulos interpretativos perante ao constante compartilhamento de conteúdo pelos usuários no mundo virtual, por vezes abrindo mão de partes da sua vida privada ao realizar publicações que possibilitam o conhecimento sobre fatos de suas vidas. Contudo, a utilização das redes de forma tão habitual, sobrepõe a normalização do consentimento ao acesso aos dados, seja para entrar em uma rede social, acessar um conteúdo pago ou até mesmo utilizar serviços em sites governamentais.

O sistema de monetização de dados e suas consequências ainda é muito desconhecido pelos indivíduos, Schreiber (2014, p. 137) assevera que a tutela da privacidade atual amplifica os contornos tradicionais do “direito a ser deixado só” para dar origem ao direito a ter controle sobre as próprias informações. Diante deste contexto, a proteção de dados passar a ser reconhecida como um direito fundamental associado à privacidade, tendo como base o poder de escolha do usuário ao permitir dispor de suas informações no ambiente tecnológico.

Os riscos advindos do consenso quase que automático ao acesso aos dados, fizeram surgir a necessidade do reconhecimento do direito a proteção de dados numa perspectiva autônoma e fundamental, tendo como base a autodeterminação afirmativa, a qual, segundo Sousa e Silva (2020, p. 11):

> [...] constitui o direito do indivíduo de decidir, em princípio, sobre o uso de dados relacionados à sua pessoa. Em outras palavras, consiste no direito do indivíduo de decidir quem utiliza, para quem são repassados e com que finalidades os dados e informações pessoais são utilizados. Essa afirmação conduz ao entendimento de que a permissão do titular em todas as fases do processamento e utilização da informação a partir do consentimento torna-se importante no momento de definir o sentido e o alcance do fundamento da autodeterminação informativa. Isto para que, o referido termo, como instrumento de exteriorização do referido fundamento, possua aplicabilidade prática e possa cumprir seu papel com eficiência.

No âmbito jurisprudencial internacional, a matéria tem como ponto principal para o início de debates, o julgamento do Tribunal Constitucional Federal da Alemanha de 15 de dezembro de 1983 (BverfGE 65,1), em que foi apurada a constitucionalidade de uma lei que estipulava o recenseamento geral da população, por meio de dados sobre suas profissões, moradia e local de trabalho dos cidadãos. Em decisão, o Tribunal considerou a necessidade do direito geral da personalidade passar a abranger a proteção do indivíduo contra levantamento, armazenamento, uso e transmissão de dados pessoais, sendo necessária a autorização, consubstanciando assim, o direito geral à autodeterminação sobre a informação, que somente é restringível se houver a contraposição de um interesse predominante da coletividade (SCHWABE, 2005, p. 233- 235).

A autodeterminação informativa é prevista na Lei Geral de Proteção de Dados Pessoais como um dos princípios basilares, buscando aferir ao titular maior proteção frente a tutela de seus dados. Existe, porém, o âmbito doutrinário, uma dissonância quanto a abrangência desse termo e sua vinculação direta com o consentimento, nesse embate Souza e Silva (2020, p. 10) asseveram ser o consentimento a exteriorização do fundamento da autodeterminação contexto prático, constituindo um elemento para sua efetivação, não quanto a elemento de construção de seu sentido.

Em contraponto, Mendes e Fonseca (2020) e Malheiro (2017) elencam ser necessário fazer a desvinculação da ideia de autodeterminação informativa baseada apenas tão somente no consentimento, considerando a associação como representante de um meio utópico e ilusório de conceitualização do termo, não atendendo os efeitos previstos, visto a relação assimétrica do uso habitual das redes e da vulnerabilidade do usuário titular dos dados ao permitir diariamente o acesso, de forma quase que automática e sem maior racionalização das consequências.

Nesse sentido, o direito à autodeterminação afirmativa não seria suficiente para prevenir o fornecimento de maneira compulsória dos dados, vez que na prática de atividade corriqueiras os indivíduos tentem a fornecer as informações como forma de acessar serviços essenciais, extrair documentos em órgãos públicos, criar contas bancárias, prestar concursos, etc. Por conseguinte, acreditar que o consentimento prévio do usuário está revestido de toda proteção da privacidade não coaduna com a realidade baseada na vasta confiança dada aos controladores dos dados, acreditando respeitarem todos os preceitos estabelecidos em lei (MOURA; ANDRADE, 2019, p. 123).

Bioni (2019, p. 116) explica que a terminologia “autodeterminação informacional” implica a interpretação equivocada de que o consentimento do titular dos dados pessoais teria primazia e prevalência na proteção dos dados pessoais, a fim de que, justamente, o sujeito autodeterminasse as suas informações pessoais.

Logo, a autodeterminação somente seria de fato exercida se as tecnologias desenvolvessem uma forma mais clara de conscientizar o titular quanto a real utilização dos dados compartilhados, de modo a participar ativamente do processo de seu tratamento. Surgindo diante deste contexto, a proposta do consentimento granular, no qual o usuário poderia ter maior discernimento quanto a quais dados seriam coletados, as modalidades, período, e qual a frequência e possibilidade de acesso por terceiros, possibilitando o consentimento de forma mais fragmentada e gradual (LUGATI E ALMEIDA, 2020, p. 201).

A implementação dessa forma de autorização de acesso aos dados se faz necessária, diante da atual chamada “crise do consentimento”, assim conceituada por Schermer, Custers e Hof (2014), os quais questionam a capacidade dos usuários possuírem protagonismo da defesa e controle dos seus dados no âmbito tecnológico. O cenário atual seria resultado da normalização do costume dos indivíduos não darem a devida importância a leitura das políticas públicas implementadas nos sites, como também da difícil forma de compressão dada pelo uso de termos técnicos do campo da informática e tecnologia, desconhecidos pela maioria dos usuários.

A sofisticação dos sistemas em conjunto com a linguagem técnica empregada, acarretam na difícil compreensão assertiva dos riscos reais oriundos do fornecimento dos dados nas redes. Destarte, para Mendes e Fonseca (2020) o consentimento seria contestável, vez que, os usuários possuem somente duas opções: consentir ou não usufruir dos serviços e informações, por vezes necessários

e essenciais. Frente a problemática, os autores apontam a materialização e monetização dos dados como soluções possíveis na responsabilização da atividade do tratamento de dados.

Outrossim, Lessig (2006) já apontava a necessidade de os governos proporem maiores articulações entre a sociedade e as empresas de tecnologia, nas áreas que dizem respeito as inovações no campo de monitoramento de dados. Ao contemplar e acompanhar a crescente modernização no sistema de coletas de dados, oferecendo maior proteção aos usuários, o setor governamental estabelece limites, regulamenta e proteger de maneira mais eficaz a tutela do direito à privacidade, reconhecendo a vulnerabilidade dos cidadãos frente a tecnologia.

Segundo Doneda (2006, p. 216) a utilização dos dados pessoais deve obedecer a finalidade comunicada ao interessado antes de sua coleta. Partindo dessa premissa, se funda a restrição da transferência dos dados pessoais coletados em dado momento, a terceiros com finalidades distintas do conhecimento do usuário no ato de consentir. A utilização dos dados fornecidos em outras relações e contextos, fora das pré-estabelecidas não podem ser validadas pelo ordenamento jurídico, por infringir claramente o direito de autodeterminação, essencial para a relação tecnológica estabelecida entre o indivíduo e provedor do serviço tecnológico oferecido.

O uso das novas tecnologias e a possibilidade do tratamento e compartilhamento de dados, como esboçado, apresentam risco à privacidade e intimidade. Segundo Doneda (2006, p. 195) um dado que em si, para o usuário, não apresenta nenhuma importância, pode adquirir um novo valor nas redes; portanto nas atuais condições de processamento automático de dados, não existe mais um dado sem importância. Por conseguinte, percebe-se a relevância de os instrumentos normativos estabelecerem garantias à privacidade e intimidade dos dados coletados e armazenados, sejam eles geridos por entidades públicas ou privadas.

5 CONCLUSÃO

No decurso do processo histórico, diversas relações complexas se consolidaram na sociedade e, junto a isso, surgem novas problemáticas que carecem de regulamentação. Uma das mais emblemáticas da atualidade é o avanço da tecnologia no mundo globalizado. As informações que antes eram restritas a espaços limitados, atualmente se difundem em uma velocidade que jamais poderia ser imaginada, derivadas das funcionalidades trazidas pelo ciberespaço.

Estar-se-á diante de dois vieses importantes e antagônicos na vida cotidiana do ser humano: de um lado as tecnologias proporcionam inúmeros benefícios, desde a prestação de serviços básicos de forma rápida e prática, proporcionando o sentimento de bem-estar aos seus usuários, de outro, promovem a interferência contínua na vida privada e no uso de dados pessoais de seus titulares.

Diante da análise aprofundada desse contexto, o desenvolvimento do presente estudo possibilitou, com base na doutrina, legislação e jurisprudência, a realização de uma investigação pormenorizada a respeito das consequências advindas do avanço tecnológico provocado pelo processo de globalização.

Como já muito bem debatido, o mundo em um “click” trouxe inúmeras facilidades aos usuários. Em verdade, é inegável os benefícios da amplificação do uso das ferramentas digitais nos diversos âmbitos da economia, especialmente no comércio digital. Entretanto, aliado a isso, surge uma nova problemática, que até então não era enfoque principal de debates recorrentes: o capitalismo de vigilância.

O termo utilizado pela professora Shoshana Zuboff (2019) evidência a celeuma em epígrafe, isto é, um novo modelo de negócios baseado na “economia de dados”. Grandes empresas de tecnologias, denominadas “*big techs*” utilizam algoritmos com o objetivo de vigiar o comportamento do usuário da rede e a partir disso capturar seus dados para definir arquétipos de hábitos e induzir ao consumo de determinadas informações e, consequentemente, produtos.

O capitalismo de vigilância se tornou um problema quando a competitividade provocou mudança no comportamento das máquinas, de modo que, ao serem “alimentadas” de informações, elas desenvolveram meios de “conhecer” os comportamentos humanos através do uso de algoritmos e a partir disso molda-los para um fim específico. Junto a isso, surgiu a necessidade de regulação dessas empresas, frente à violação de alguns direitos fundamentais.

Frente a esse novo cenário, tornou-se imprescindível à amplificação de ferramentas de proteção de direitos fundamentais, especialmente os da privacidade e proteção de dados dos usuários, considerados pela doutrina como de quarta dimensão, visto que não é difícil imaginar que o digital traz inúmeras ameaças e preocupações aos bens jurídicos por eles tutelados.

A privacidade, antes adstrita a intimidade e inviolabilidade de domicílio, ganha novos contornos com a era digital. As novas modalidades de consumo de produtos e serviços no ciberespaço refletiu mudanças na captação e armazenamento de dados. Isso ressoa a possibilidade de ofensa dessa garantia constitucional, tendo em vista que para ter acesso à rede e a tudo que ela proporciona, o usuário é levado a compartilhar informações pessoais.

Em verdade, não há como discordar que a sociedade da informação e tudo que ela engloba é o centro dos principais debates no século XXI. As discussões acerca das transformações sociais que alteraram todo o contexto do processo de globalização, especialmente a partir do advento das Tecnologias da Informação e Comunicação (TICs), que quebraram fronteiras em todo o mundo, se intensificaram nos últimos anos.

Esse novo cenário desencadeou a necessidade de uma legislação específica para tutelar os bens jurídicos afetados pelas novas nuances trazidas pela sociedade da informação.

Inicialmente, em se tratando do âmbito nacional, a pesquisa cita a Lei nº 12.965 publicada em 23 de abril de 2014, que já estabelecia princípios, garantias, direitos e deveres para o uso da internet no Brasil. Entretanto, em virtude das novas conjunturas sociais que surgiram com o desenvolvimento tecnológico, o legislador achou por bem criar a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709 de 2018 que entrou em vigor em agosto de 2020, inspirada no Regulamento Geral de Proteção de Dados Europeu (RGPD). A nova lei amplificou o rol de proteção de direitos, trazendo em seu arcabouço a égide da liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Ao analisar a Lei Geral de Proteção de Dados, foi perceptível que o legislador deu grande ênfase a ideia de consentimento. O consentimento simboliza mecanismo de manifestação individual da autodeterminação informativa e autonomia da vontade no campo dos direitos da personalidade, e tem por objetivo de validar o uso de dados

por terceiros. Em regra, isso se concretiza quando o usuário aceita os termos de uso de cookies de determinada plataforma na rede.

Ao se conectar a um endereço eletrônico e consentir com as disposições inseridas na política de cookies, o usuário, na teoria, estará anuindo com seus termos. Isso faz com que haja exposição dos dados, que são compartilhados e até mesmo usados como insumo para o comércio respaldado no capitalismo de vigilância.

A LGPD conceitua o termo “consentimento” como: a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. O consentimento, na legislação pátria, está diretamente atrelado aos princípios da informação e da boa-fé objetiva, elencado no art. 6º, caput, da LGPD.

Assim, a partir da adesão aos termos inseridos nos cookies, os dados são coletados sem que o indivíduo que navega tenha conhecimento de como serão utilizados. Nem sempre, ou melhor, quase nunca o titular de dados possui cognição do que aceita. Além disso, observa-se um desequilíbrio de poderes entre o usuário e o agente tratador de dados, característico das relações consumeristas. Logo, é incerto que o indivíduo tenha pleno gerenciamento dos riscos inerentes a essa prática.

O capitalismo de vigilância que, por si só, já era uma problemática discutida por diversos especialistas por causar inúmeras consequências negativas para a sociedade, se agravou a partir do momento que as grandes empresas passaram a utilizar o consentimento como forma de fundamentar a sua legitimidade.

No entanto, a complexidade do atual contexto da sociedade da informação não permite que o titular seja o único responsável pela proteção de dados pelo simples consentir. Desse modo, a responsabilidade deve ser compartilhada entre todos os agentes, especialmente aqueles que estão na cadeia de maior hierarquia frente a notável vulnerabilidade existente entre usuário e tratador.

Dessa maneira, Mendes e Fonseca (2020, p. 526) trazem algumas soluções possíveis para que o capitalismo de dados seja realizado de forma legítima, sem haver a violação de direitos fundamentais (ou para que haja uma paridade de armas entre usuário e tratador), quais sejam, a tecnologia e o desenho dos sistemas informacionais (privacy by design), que podem auxiliar o titular no controle de seus dados; um sistema robusto de prestação de contas pelos agentes de tratamento (accountability), apto a dimensionar os riscos prévios ao tratamento de dados pessoais; e, por fim, o controle substantivo e contextual do consentimento.

Além disso, não se pode olvidar a necessidade de agregar a todo e qualquer movimento de coleta e tratamento de dados as outras inúmeras disposições previstas na LGPD, especialmente os seus princípios norteadores, que dão azo a uma maior segurança jurídica para a sociedade da informação. Portanto, se aplicada de forma correta, a LGPD pode ser considerada como um marco regulatório eficaz para o combate a problemática gerada pelo capitalismo de vigilância.

Em tempo, considera-se que o ritmo crescente da economia baseada na informação reflete em aspectos jurídicos, uma vez que esse novo paradigma está diretamente atrelado à violação de direitos fundamentais. Desse modo, a partir do momento em que o capitalismo passa a estar minerado na coleta de dados, a sociedade e o Poder Público, no campo do ser, necessitam estar preparados para enfrentar e assumir uma posição diante das transformações oriundas desse novo contexto, especialmente quando se trata da prevenção e reparação dos efeitos negativos.

REFERÊNCIAS BIBLIOGRÁFICAS

ACQUISITI, Alessandro. **Nudging privacy: The behavioral economics of personal information.** IEEE Security & Privacy v. 7, n. 6, pp. 82–85, 2009.

ALDEIAS, Marisa. **Cookies: uma ameaça à privacidade.** 2012. Disponível em < https://silo.tips/queue/cookies-uma-ameaa-a-privacidade-2?&queue_id=-1&v=1704515566&u=MTcwLjc5LjUuMjU1> Acesso em 25 nov. 2023.

ALEXY, Robert. **Teoria dos direitos fundamentais**. São Paulo: Malheiros, 2008.

ALBERS, Marion. **Realizing the Complexity of Data Protection. In: GUTWIRTH, Serge; LEENES, Ronald; HERT, Paul De. (Edit.)**. Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges. Berlin: Springer, 2014.

AYRES, Ian; BRAITHWAITE, John. **Responsive Regulation: Trancending the Deregulation Debate.** New York: Oxford. Oxford University Press. 1992.

BALKIN, Jack M. **Fixing Social Media's Grand Bargain. Hoover Working Group on National Security Technology, and Law, Aegis Paper Series n. 1814**, October 2018.

BASTOS, Celso Ribeiro. **Curso de direito constitucional**. 21ª.ed. São Paulo: Saraiva, 2000.

BASTOS, Celso Ribeiro; MARTINS, Ives Gandra. **Comentários à Constituição do Brasil***.* São Paulo: Saraiva, 1989, vol. 2, p. 63.

BAUMAN, Zygmunt. **Modernidade Líquida.** Rio de Janeiro: Zahar, 2013.

BEIRIZ; LANNES; NICHELLI; MENDES, FERREIRA; SALGADO; SIQUEIRA; PRATA. **REGULAÇÃO DAS BIG TECHS: o que dizem os atores envolvidos?** Instituto de Relações Internacionais: PUCRIO, 2021. Disponível em < https://www.puc-rio.br/ensinopesq/ccpg/pibic/relatorio_resumo2021/download/relatorios/CCS/IRI/IRI_Bernardo%20Beiriz;Daniel%20Lannes;Juliane%20Nichelli;Maria%20Clara%20Mendes;Nathan%20Ferreira.pdf > Acesso em 02 jun. 2023.

BELL, Daniel. **O advento da sociedade pós-industrial: uma tentativa de previsão social.** Trad. Heloysa de Lima Dantas. São Paulo: Cultrix, 1973.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento.** Rio de Janeiro: Forense, 2019.

BITTAR, Carlos Alberto. **Os direitos da personalidade**. 6a ed. rev., atual. e ampl. de acordo como o novo Código Civil. Rio de Janeiro: Forense Universitária, 2003.

BOBBIO, Norberto. **A Era dos Direitos**. 13ª Reimpressão. Rio de Janeiro: Editora Elsevier, 2004.

BOBBIO, Norberto. **A Era dos Direitos**. Rio de Janeiro: Editora Elsevier, 1992.

BOBBIO, Norberto. **A Era dos Direitos.** Trad.: Carlos Nelson Coutinho. Rio de Janeiro: Elsevier, 2004b.

BONAVIDES, Paulo. **Curso de Direito Constitucional**. 19ª Edição, São Paulo: Editora Malheiros, 2006.

BORGES, Rosa Maria Zaia. **Democracia, Liberdade de expressão e Black Blocs.** Rev. Direito e Práx., Rio de Janeiro, Vol. 08, N. 1, 2017, p. 354-385. Disponível em < https://www.scielo.br/j/rdp/a/74ycpg5wJQwZB7PLdCQ8Ggd/?lang=pt&format=pdf> Acesso em 01 de fevereiro de 2024.

BRAITHWAITE, J. John Braithwaite. **UBC Law Review**, Vancouver, 44, n. 3, 2011. 475-520.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 2630, de 2020**. Relatório n. 1/2021 do Grupo de Trabalho para aperfeiçoamento da legislação brasileira referente à liberdade, responsabilidade e transparência na internet. Relator: Dep. Orlando Silva, 28 de outubro de 2021. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2097604&filename=Tramitacao-PL+2630/2020. Acesso em: 02 jun. 2023.

BRASIL. **Medida Provisória n° 1068, de 06 de setembro 2021**. Altera a Lei nº 12.965, de 23 de abril de 2014, e a Lei nº 9.610, de 19 de fevereiro de 1998, para dispor sobre o uso de redes sociais. Brasília: Presidência da República, 2021. Disponível em: https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/149726. Acesso em: 02 jun. 2023.

BRASIL. Marco Civil da Internet. **Lei 12.964/14**. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm >. Acesso em: 23 jan. 2024.

BRASIL**. Lei nº 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm. Acesso em: 14 dez. 2023.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidente da República, [2016]. Disponível

em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 02 fev. 2023.

BRASIL. **Decreto nº 8771/16** de 11 de maio de 2016. Diário Oficial da República Federativa do Brasil. Brasília, DF, 11 maio 2016. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm. Acesso em 28. out. 2023.

BULOS, Uadi Lammêgo. **Curso de Direito Constitucional**. 3. ed. São Paulo: Saraiva, 2007.

BULOS, Uadi Lammêgo. **Curso de Direito Constitucional**. São Paulo: Saraiva, 2007.

CACHAPUZ, M. C. **Intimidade e vida privada no novo Código Civil Brasileiro:** uma leitura orientada no discurso jurídico. Porto Alegre: Sergio Antônio Fabris Ed., 2006.

CAETANO, João Victor Lima. **O Regulamento Geral de Proteção de Dados (GDPR): Uma Análise Extraterritorial Scope à Luz da Jurisdição Internacional.** Cadernos Eletrônicos Direito Internacional sem Fronteiras, Vol. 2, Núm. 1, Jan-Jun 2020, e:11.

CAHN, Aaron. ALFELD, Scott. BARFORD, Paul. MUTHUKRISHNAN, S. **An Empirical Study of Web Cookies. 25th International Conference on World Wide Web (WWW '16),** International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, Switzerland, pp. 891-901. DOI: .

CARVALHO, Mariana Amaral. **Capitalismo de Vigilância: a privacidade na sociedade da informação.** Dissertação de Mestrado – Universidade Federal de Sergipe. Aracaju. 2019.

CASTELLS, M. **A sociedade em rede**. São Paulo: Paz e Terra, 2001.

CASTELLS, Manuel; CARDOSO, Gustavo (Org.). **A sociedade em rede:** do conhecimento à acção política. Brasília: Imprensa Nacional-Casa da Moeda: 2006, p. 17-30.

CASTELLS, Manuel. **A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade**. Rio de Janeiro: Jorge Zahar editor, 2003.

CASTELLUCCIA, Claude**. Behavioural Tracking on the Internet: A Technical Perspective.** In: GUTWIRTH, Serge et al. (eds). European Data Protection: Good Health? Dordrecht: Springer, 2012.

CONSUMERS INTERNATIONAL, Coming Together for Change. **The State of Data Protection Rules around the World: a briefing for consumer organisations.** Disponível em: Acesso em: 02/12/2019.

COSTA JÚNIOR, Paulo José da. **O direito de estar só: tutela penal da intimidade.** 3ª ed. São Paulo: Siciliano Jurídico, 2004.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de dados pessoais comentada.** 2. ed. São Paulo: Revista dos Tribunais, 2019.

DEMO, Pedro. Ambivalências da sociedade da informação. **Ci. Inf**., Brasília, v. 29, n. 2, Aug. 2000.

DENLEY, Andrew; et al. **GDPR: How to Achieve and Maintain Compliance.** New York. Routledge Publishing. 2018, 257 p.

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

EVANGELISTA, Rafael de Almeida. **Capitalismo de vigilância no sul global: por uma perspectiva situada.** In: SIMPOSIO INTERNACIONAL LAVITS VIGILANCIA, DEMOCRACIA Y PRIVACIDAD EM AMÉRICA LATINA: VULNERABILIDADES Y RESISTÊNCIAS, 5., Santiago, Chile, dez. 2017. Anais [...]. Santigado, 2017. p. 243-253. Disponível em: http://lavits.org/wpcontent/uploads/2018/04/08-Rafael-Evangelista.pdf. Acesso em: 12 jan. 2021.

FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani (coords.). **Comentários à lei geral de proteção de dados: Lei 13.709/2018**. São Paulo: Revista dos Tribunais, 2019.

FERRAZ JUNIOR, Tércio Sampaio. **Sigilo de dados:** o direito à privacidade e os limites à função fiscalizadora do Estado. Cadernos de direito constitucional e ciência política, ano 1. São Paulo: *Revista dos Tribunais*, 1993.

FINKELSTEIN, Maria Eugênia; FINKELSTEIN, Claudio. **Privacidade e a Lei Geral de Proteção de Dados.** Florianópolis: Revista de Direito Brasileira, 2019.

FLAHERTY, David H. On the utility of constitutional rights to privacy and data protection. **Case Western Reserve Law Review**, 1990-1991, v. 41, pp. 831-855.

FORNASIER, Mateus de Oliveira; FERREIRA, Luciano Vaz. **A autorregulação e direito global: os novos fenômenos jurídicos não-Estatais**. In: Revista do Programa de PósGraduação em Direito da UFC, vol. 35.2, jul./dez. de 2015.

FORNASIER, Mateus de Oliveira; BECK, Cesar. Cambridge Analytica: escândalo, legado e possíveis futuros para a democracia. Revista Direito em Debate, ano XXIX, v. 29, n. 53, p. 182- 195, jan./jun. 2020. Disponível em: https://www.revistas.unijui.edu.br/index.php/revistadireitoemdebate/article/view/10033. Acesso em: 10 out. 2023.

FRANÇA, Lilian Cristina Monteiro. **Vigilância e políticas de privacidade na sociedade pós-cookie: O caso do The Guardian.** Revista Eco Pós, v. 18, n. 2, p. 95-105, 2015. Disponível em: https://uakari.org.br/eco_pos/article/view/2229. Acesso em: 25 nov. 2023.

FRAZÃO, Ana. **Capítulo 1** – Fundamentos da Proteção dos dados pessoais – Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: FRAZÃO, Ana; OLIVA. Milena Donato; TEPEDINO, Gustavo. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, edição digital sem numeração de página.

FRAZÃO, Ana. **Capítulo 4** – Objetivos e alcance da Lei Geral de proteção de Dados. In: FRAZÃO, Ana; OLIVA. Milena Donato; TEPEDINO, Gustavo. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** São Paulo: Thomson Reuters Brasil, 2019, edição digital sem numeração de página.

FREDES, Andrei; BORGES, Mariana. **Revista Direitos Democráticos & Estado Moderno**. Faculdade de Direito da PUC-SP. DD&EM nº 02, p.181-195, Jan-Jun.2021.

FROTA, Hidemberg Alves da. **A proteção da vida privada, da intimidade e do segredo no Direito brasileiro e Comparado.** Anuario de Derecho Constitucional Latinoamericano, Montevideo, v. 13, n. 1, t. 2, p. 459-495, ene.-dic. 2007.

FUCHS, Christian. **Class and Exploitation on the Internet.** In: Trebor Sholz (org.). Digital Labor: The Internet as Playground and Factory. New York: Routledge, 2013.

GIANNASI, Maria Júlia. **O profissional da informação diante dos desafios da sociedade atual**. Brasília, 1999. Tese (Doutorado) - Universidade de Brasília, Brasília.

GONÇALVES, Leonardo Fernandes. **Análise da política de cookies sob a ótica da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18).** 2022. Disponível em < https://pantheon.ufrj.br/bitstream/11422/20630/1/LFGon%c3%a7alves.pdf>. Acesso em 01 jan. 2023.

HARARI, Yuval Noah. **21 lições para o século 21**. Tradução Paulo Geiger. São Paulo: Companhia das Letras, 2018.

HOOFNAGLE, Chris Jay; URBAN, Jennifer M.; LI, Su**. Privacy and modern advertising: most US internet users want 'do not track' to stop collection of data about their online activities**. In: AMSTERDAM PRIVACY CONFERENCE, 2012. HOOFNAGLE, Chris Jay; SOLTANI, Ashkan; GOOD, Nathan; WAMBACH, Dietrich James; AYENSON, Mika. Behavioral advertising: the offer you cannot refuse. Harvard Law & Policy Review, v. 6, p. 273, Aug. 2012); UC Berkeley Public Law Research Papern. 2137601, p. 273-296 apud BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. p. 151.

HUBMANN, Heinrich. Das persönlichkeitsrecht. Münster: Böhlau-Verlag, 1953, p. 30-40.

HUBMANN, Heinrich. Das Persönlichkeitsrecht. Böhlnau – Verlag Münster / Köln, 1967.

IRAMINA, A. **RGPDv. LGPD:** Adoção Estratégica da Abordagem Responsiva na Elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento Geral de Proteção de Dados da União Europeia. Revista de Direito, Estado e Telecomunicações, Brasília, v. 12, nº 2, p. 91-117, Outubro de 2020.

JABUR, Gilberto Haddad. **Liberdade de pensamento e direito à vida privada.** Conflitos entre direitos da personalidade. São Paulo: RT, 2000. p. 253-254.

KHONDKER, Habibul Haque. "Glocalization as globalization: evolution of a sociological concept". Bangladesh e-Journal of Sociology, vol. 1, nº 2, 2004, pp. 1-9.

LAMBRINOUDAKIS, Costos; VIMERCATI, Sabrina. (Edit.). Digital Privacy: Theory, Technologies, and Practices, Boca Raton: Auerbach Publications, 2007.

LAWAND, Jorge José. **Teoria geral dos contratos eletrônicos**. São Paulo: Editora Juarez de Oliveira, 2003, p. 103.

LEE, Sangwoo. **A Study on the Extraterritorial Application of the General Data Protection Regulation with a Focus on Computing. PHD Dissertation. (Phd in International Law)**. China University of Political Science and Law. Beijing. 2018, 539 p.

LESSIG, Lawrence. **Code Version 2.0**. Nova Iorque: Basic Books, 2006.

LÉVY, Pierre. **Cibercultura**. Trad de Carlos Irineu da Costa. 1 ed. Ed 34. São Paulo, 1999.

LIMBERGER, Têmis. Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação Pública (LAI) um diálogo (im)possível? As influências do Direito Europeu. **REVISTA DE DIREITO ADMINISTRATIVO**, v. 281, p. 113-144, 2022.

LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de. **Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa.** Revista de Direito, Viçosa, v. 12, n. 2, p. 1-33, 2020. Disponível em: https://periodicos.ufv.br/revistadir/article/view/10597. Acesso em: 20 nov.2023.

MACEDO JÚNIOR, Ronaldo Porto. **Privacidade, mercado e informação.** Justitia, São Paulo, v. 61, n. 185/188, pp. 245-259, jan./dez. 1999.

MACHADO, J.; MISKOLCI, R. **Das jornadas de junho à cruzada moral: o papel das redes sociais na polarização da política brasileira**. Revista Sociologia & Antropologia, Rio de Janeiro, v. 9, n. 3, p. 945-970, set./dez. 2019. DOI: https://doi.org/10.1590/2238-38752019v9310. Disponível em: https://www.scielo.br/j/sant/a/q8zsjyJYW3Jf3DBFSzZJPBg/?lang=pt. Acesso em: 16 mai. 2023.

MALHEIRO, Luíza Fernandes. **O consentimento na proteção de dados pessoais na Internet: uma análise comparada do regulamento geral de proteção de dados europeu e do projeto de lei 5.276/2016. 2017**. 86 f. Trabalho de Conclusão de Curso (Graduação em Direito) – Faculdade de Direito, Universidade de Brasília, Brasília, 2017. Disponível em: https://bdm.unb.br/bitstream/10483/18883/1/2017_LuizaFernandesMalheiro.pdf. Acesso em: 4 nov. 2023.

MARINONI, Luiz Guilherme. MITIDIERO, Daniel. SARLET, Ingo Wolfgang. **Curso de Direito Constitucional.** São Paulo: Editora Revista dos Tribunais, 2017.
MARMELSTEIN, George. **Curso de direitos fundamentais.** São Paulo: Altas, 2008.

MARQUES, Claudia Lima. **Boa-fé nos serviços bancários, financeiros de crédito e securitários e o Código de Defesa do Consumidor: informação, cooperação e renegociação?.** Revista da Faculdade de Direito, Porto Alegre, 2002. Disponível em: https://seer.ufrgs.br/revfacdir/article/view/72637/41109. Acesso em: 02 de julho de 2023.

MARQUES, Claudia Lima. **Boa-fé nos serviços bancários, financeiros de crédito e securitários e o Código de Defesa do Consumidor:** informação, cooperação e renegociação?. Revista da Faculdade de Direito, Porto Alegre, 2000. Disponível em: https://seer.ufrgs.br/revfacdir/article/view/72637/41109. Acesso em: 02 de julho de 2023.

MARQUES, Claudia Lima; MIRAGEM, Bruno. **O Novo Direito Privado e a Proteção dos Vulneráveis**. São Paulo: Revista dos Tribunais, 2012.

MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura. **A anonimização de dados pessoais: consequências jurídicas do processo de reversão, a importância da entropia e sua tutela à luz da Lei Geral de Proteção de Dados.** In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (Coord.). Direito & Internet IV: sistema de proteção de dados pessoais. São Paulo: Quartier Latin, 2019.

MARTINS, Helena. **Entenda o Marco Civil da Internet**. Agência Brasil, 2014. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2014-04/entenda-o-marco-civil-da-internet. Acesso em: 16 dez. 2022.

MARTINS-COSTA, Judith. **A boa-fé no direito privado**. 2. ed. São Paulo: Saraiva Educação, 2018.

McNAIR, B. **Fake news: falsehood, fabrication and fantasy in journalism.** London: Routledge, 2017.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional**. 15. ed. São Paulo: Saraiva, 2012.

MENDES, Gilmar Ferreira. **Curso de direito constitucional** / Gilmar Ferreira Mendes, Paulo Gustavo Gonet Branco. – 7. ed. rev. e atual. – São Paulo : Saraiva, 2012.

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

MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. **Proteção de dados para além do consentimento: tendências contemporâneas de materialização**. Revista Estudos Institucionais, v. 6, n. 2, p. 507-533, maio/ago. 2020. Disponível em: https://www.estudosinstitucionais.com/REI/article/view/521. Acesso em: 5 nov. 2023.

MILNE, George R; CULNAN, Mary J. **Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices**. Journal of Interactive Marketing, v. 18, issue 3, pp. 15-29, 2004.

MIRAGEM, Bruno. **A Lei Geral de Proteção de dados (Lei 13.709/2018) e o direito do consumidor.** Revista dos Tribunais, v. 1009, Nov., 2019. Disponível em: https://www.brunomiragem.com.br/wp-content/uploads/2020/06/002-LGPD-e-o-direito-doconsumidor.pdf. Acesso em: 01 de julho de 2023.

MOURA, Plínio Rebouças; ANDRADE, Diego Calasans Melo. **O direito de consentimento prévio do titular para o tratamento de dados pessoais no ciberespaço.** Revista de Direito, Governança e Novas Tecnologias, v. 5, n.1, p. 110-133, jan./jun. 2019. Disponível em: https://www.indexlaw.org/index.php/revistadgnt/article/view/5568. Acesso em: 20 nov. 2023.

MORAIS, Leonardo Stoll de. DIREITO À PRIVACIDADE NO SISTEMA REGIONAL EUROPEU DE DIREITOS HUMANOS. **Revista de Direito Brasileira** | Florianópolis, SC | v. 25 | n. 10 | p. 200-220 | Jan./Abr. 2020.

MORAIS, Leonardo Stoll de. Direito a Privacidade no Sistema Regional Europeu de Direitos Humanos. Revista de Direito Brasileira | Florianópolis, SC | v. 25 | n. 10 | p. 200-220. Disponível em < https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj7zNTExbKEAxXhgWEGHXMlCGcQFnoECA8QAQ&url=https%3A%2F%2Fwww.indexlaw.org%2Findex.php%2Frdb%2Farticle%2Fdownload%2F3902%2F5072&usg=AOvVaw2G8ffi3P5q8QF2JqLimPyB&opi=89978449> Acesso em: 14 dez. 2023.

NADLER. Jerrold, CICILLINE. David N; **Investigation Of Competition In Digital Markets: Majority Staff Report And Recommendations Subcommittee On Antitrust Commercial And Administrative Law Of The Committee On The Judiciary** – 2020. pp-174.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. **Myths and fallacies of "personally identifiable information"**. Communications of the ACM, Nova York, v. 53, n. 6, p. 24-26, 2010. Disponível em: http://bit.ly/30G9CVq. Acesso em: 23 ago. 2022.

NAVARRO, Ana Maria Neves de Paiva. **Privacidade Informacional:** origem e Fundamentos no Direito Norte-Americano. Publica Direito. Disponível em < http://www.publicadireito.com.br/artigos/?cod=34f9a343f945196b>. Acesso em 05 de maio de 2023.

NOHARA, I. P. Desafios da ciberdemocracia diante do fenômeno das Fake News: regulação estatal em face dos perigos da desinformação. In: RAIS, D. (coord.). **Fake news**: a conexão entre a desinformação e o direito. São Paulo: Thomson Reuters Brasil, 2018. p. 75-88.

NORMAN, Jeremy. **Louis Montulli II Invents the HTTP Cookie**. Disponível em: https://www.historyofinformation.com/detail.php?id=2102. Acesso em: 02 dez. 2023.

NOVELINO, Marcelo. **Direito Constitucional**. 2.ed. Rev. Atual. e ampl. São Paulo: Método, 2008.

NOVELINO, Marcelo. **Curso de Direito Constitucional.** 12ªed. - revista, atualizada e ampliada. Salvador: JusPODIVM, 2017.

O'NEILL, Cathy. **Weapons of math destruction:** How Big Data Increases Inequality and Threatens Democracy. NY: Brodway Books, 2016.

OHCHR. **Human rights in the digital age - Can they make a difference? Keynote speech by Michelle Bachelet, UN High Commissioner for Human Rights**. Japan Society, New York, 17 October 2019.

OLIVEIRA, Jordan Vinícius de; SILVA, Lorena Abbas da. **Cookies de computador e história da internet: desafios à lei brasileira de proteção de dados pessoais.** Revista de Estados Jurídicos UNESP, ano 22, n. 36, p. 307-388, 2018. Disponível em: https://periodicos.franca.unesp.br/index.php/estudosjuridicosunesp/article/view/2767. Acesso em: 20 nov. 2023.

PAESANI, Liliana Minardi. Direito e Internet. **Liberdade de informação, privacidade e responsabilidade civil.** 7. ed. São Paulo: Atlas, 2014.

PASQUALE, Frank. **The black box society. The secret algorithms that control money and information.** Cambridge: Harvard University Press, 2015.

PARDO, David Wilson de Abreu. **Para uma interpretação conforme os direitos fundamentais.** Universidade Federal de Santan Catarina - UFSC: Florianópolis, 1998. Disponível em https://repositorio.ufsc.br/bitstream/handle/123456789/77404/137745.pdf?sequence=1&isAllowed=y. Acesso em 19 de julho de 2023.

PEREIRA, Marcelo Cardoso. **Direito à intimidade na internet**. 2ª ed. Curitiba: Juruá Editora, 2004.

PÉREZ LUÑO, Antonio Enrique. **Derechos Humanos, Estado de Derecho y Constitución**. 6. ed. Madrid: Tecnos, 1999.

PEREZ LUNO, Antonio Enrique. **Los derechos fundamentales**. Madrid: Tecnos, 2004.

PIRES, A. C. M.; PIRES, L. R. G. M. **Desinformação: atuação do Estado, da sociedade civil organizada e dos usuários da internet. In: RAIS, D. (coord.). Fake news: a conexão entre a desinformação e o direito.** São Paulo: Thomson Reuters Brasil, 2018. p. 89-104.

PRATES, Cristina Cantú. Privacidade e intimidade na Internet: a legalidade dos cookies e spam. FMU DIREITO: Revista Eletrônica, v. 28, n. 42, 2014. Disponível em: https://revistaseletronicas.fmu.br/index.php/FMUD/article/view/676. Acesso em: 20 nov. 2023.

SAMPAIO, José Adércio. **Direito à intimidade e à vida privada: uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte**. Belo Horizonte: Del Rey, 1998.

SANTANA, Karla Thais Nascimento; SILVA, Lucas Gonçalves da; SILVA, Rennan Gonçalves. **Discurso do ódio x direito à liberdade de expressão: uma análise sobre os desafios do combate à homofobia nas redes sociais.** Anais CONPEDI. 2022. Disponível em: http://site.conpedi.org.br/publicacoes/465g8u3r/83gwnf91/D7Kv92YJg6UPEG1B.pdf. Acesso em: 14 de outubro de 2022.

SANTIN, Janaína Rigo; PRA, Marlon Dai. **Relações de poder e democracia: como regular a desinformação no ecossistema das big-techs.** V. 27, N 2. Revista Pensar: Fortaleza, 2022. Disponível em <https://ojs.unifor.br/rpen/article/view/11442/6823>. Acesso em 01 jun. 2023.

SANTIN, Janaína Rigo; PRA, Marlon Dai. **Relações de poder e democracia: como regular a desinformação no ecossistema das big-techs.** V. 27, N 2. Revista Pensar: Fortaleza, 2022. Disponível em <https://ojs.unifor.br/rpen/article/view/11442/6823>. Acesso em 01 jun. 2023.

SARLET, Gabrielle Bezerra Sales; RODRIGUEZ, Daniel Piñeiro. **A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E OS DESAFIOS TECNOLÓGICOS:** ALTERNATIVAS PARA UMA ESTRUTURAÇÃO RESPONSIVA NA ERA DA GOVERNANÇA DIGITAL. Rev. direitos fundam. democ., v. 27, n. 3, p. 217-253, set./dez. 2022.

SARLET, Ingo Wolfgang. **A Eficácia dos Direitos Fundamentais.** 8ª Edição, Porto Alegre: Livraria do Advogado Ed., 2007.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme. MITIDIERO, Daniel. **Curso de Direito Constitucional**. 6. ed. São Paulo: Saraiva, 2017.

SCHREIBER, Anderson. **Direitos da personalidade.** 2. ed. rev. e atual. São Paulo: Atlas, 2013.

SCHREIBER, Anderson. **Direitos da personalidade**. 3. ed. São Paulo: Atlas, 2014.

SCHWABE, Jürgen. **50 anos de jurisprudência do Tribunal Federal Constitucional Alemão.** Tradução: Beatriz Hennig et all. Montevidéu: Fundacion Konrad-Adenauer, 2005. Disponível em: 10 out. 2023.

SCHERMER, Bart Willem; CUSTERS, Bart; HOF, Simone, van der. **The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection.** Ethics and Information Technology, 2014. Disponível

em:https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412418#references-widget. Acesso em: 20.nov.2023.

SEABROOK, Jeremy. **The Leisure Society.** Oxford: Blackwell, 1988.

SILVA, Adriana Vasconcelos de Paula. **Desafios na regulação de Big Techs e como a Teoria da Regulação Responsiva pode auxiliar na solução.** Revista de Direito Setorial e Regulatório, v. 8, nº 2, p. 95-113, outubro 2022.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 39º ed. São Paulo: Malheiros Editores, 2016.

SILVA, Lucas Gonçalves da; DETONI, Andrea Galvão Rocha. **A proteção dos direitos fundamentais à luz da sociedade da informação.** In: PORTELA, Irene (Dir.) O Direito Constitucional e o seu papel na construção do cenário jurídico global. Barcelos: Instituto Politécnico do Cávado e do Ave, 2016.

SILVA, Lucas Gonçalves da; SIQUEIRA, Alessandra Cristina de Mendonça. A (HÁ) LIBERDADE DE EXPRESSÃO NA SOCIEDADE EM REDE (?): MANIPULAÇÃO NA ERA DIGITAL. **Relações Internacionais no Mundo Atual**, v. 2, n. 23, p. 195-217, 2019.

SIMÕES, Isabella de Araújo Garcia. A sociedade em Rede e a Cibercultura: dialogando com o pensamento de Manuel Castells e de Pierre Lévy na era das novas tecnologias de comunicação. **Revista eletrônica Temática**. ano V, n. 05 ,maio 2009. Disponível em: www.insite.pro.br. Acesso em: 15 mar. 2023.

SIQUEIRA JUNIOR, Paulo Hamilton. **Teoria do Direito**. 3. ed. São Paulo: Editora Saraiva, 2012.

SOLOVE, Daniel J. **Privacy Self-Management and the Consent Dilemma**. Harvard Law Review, v. 126, pp. 1880-1903, 2013.

SOLOVE, Daniel J. The Myth of the Privacy Paradox. GWU Legal Studies Research Paper no. 2020-10, 2020. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3536265 Acesso: 10 de janeiro de 2024.

SOUZA, Carlos Affonso; LEMOS, Ronaldo; BOTTINO, Celina. **Marco Civil da Internet: jurisprudência comentada.** São Paulo: Revista dos Tribunais, 2017.

SOUSA, Rosilene Paiva Marinho de; SILVA, Paulo Henrique Tavares da. **Proteção de dados pessoais e os contornos da autodeterminação informativa. Informação & Sociedade**: Estudos, João Pessoa, v. 30, n. 2, p. 1-19, abr./jun. 2020.

Disponível em: https://periodicos.ufpb.br/ojs2/index.php/ies/article/view/52483. Acesso em: 10 out. 2023.

STEGMANN, Andreas. **What is (Big) Tech? A Taxonomy**. (Março 3, 2020). Disponível em: https://medium.com/hyperlinked/what-is-big-tech-a-taxonomy-af17c3aff88d. Acesso em: 15 mai. 2023.

SUPREMO TRIBUNAL DE JUSTIÇA. **É abusiva cláusula que obriga cliente de cartão de crédito a fornecer dados a terceiros.** Portal do STJ, 2017. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias-antigas/2017/2017-11-09_08-03_E-abusivaclausula-que-obriga-cliente-de-cartao-de-credito-a-fornecer-dados-a-terceiros.aspx. Acesso em: 03 dez. 2023.

TAMBINI, D.; MOORE, M. **Regulating Big Tech**. 1. ed. Nova Iorque: Oxford University Press, 2022.

TAKAHASHI, T. (Org). **Sociedade da informação no Brasil:** livro verde. Brasília: Ministério da Ciência e Tecnologia, 2000. Disponível em: https://www.governodigital.gov.br/documentose-arquivos/livroverde.pdf. Acesso em: 11 fev. 2023.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini. **Consentimento e proteção de dados pessoais na LGPD**. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados pessoais e sua repercussão no direito brasileiro. São Paulo: Ed. RT, 2019, p. 300.

TOBBIN, Raissa Arantes; CARDIN, Valéria Silva Galdino**. Política de cookies e a "crise do consentimento": Lei Geral de Proteção de Dados e a autodeterminação informativa.** Revista da Faculdade de Direito da UFRGS, Porto Alegre, n. 47, p. 241-262, dez. 2021. DOI: https://doi.org/10.22456/0104-6594.113663

TONIAZZO, Daniela Wendt. O CONSENTIMENTO NA LEI GERAL DE PROTEÇÃO DE DADOS E O PROBLEMA DA ASSIMETRIA INFORMACIONAL: SOLUÇÕES A PARTIR DA CLÁUSULA GERAL DA BOA-FÉ OBJETIVA. Mestrado em Direito. Pontifícia Universidade Católica do Rio Grande do Sul: Porto Alegre, 2022. Disponível em < https://tede2.pucrs.br/tede2/bitstream/tede/10358/2/DANIELA_WENDT_TONIAZZO.pdf> Acesso em 23 de dezembro de 2023.

VARELLA, Marcelo Dias. **Internacionalização do direito: Direito internacional, globalização e complexidade.** Brasília: UniCEUB, 2013.

VAINZOF, Rony. **Dados pessoais, tratamento e princípios**. In. MALDONADO, Viviane Nobrega; BLUM, Renato Opice (Coord.). Comentários ao GDPR;

Regulamento Geral de Proteção de Dados da União Europeia - São Paulo: Thomson Reuters Brasil, 2018, p. 37- 81.

VERMEULEN, Gert; LIEVENS, Eva. **Data Protection and Privacy under Pressure. Antwerp.** Maklu Publishing. 2017, 341 p.

WIENER, Norbert. **Cibernética e sociedade: o uso humano de seres humanos.** São Paulo: Cultrix, 1984.

WIENER, Norbert. **Cybernetics: or the control and communication in the animal and the machine**. Massachusetts Institute of Technology, 1948.

ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância**. Editora Intrínseca Ltda, Rio de Janeiro, 2021.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância:** a luta por um futuro humano na nova fronteira do poder. Tradução George Schlesinger. 1. ed. Rio de Janeiro: Intrínseca, 2020.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism. The fight for a human future at the new frontier of power.** New York: Public Affairs, 2019.

ZUQUIM, Pedro Cese Caram. 2021. **A Expansão das Big Techs nos Mercado Digital e Killer Acquisitions.** Monografia Final de Curso, Faculdade de Direito, Universidade de Brasília, Brasília, DF, número de páginas p. 80.